Phrack RU issue 040

Русская версия Phrack, выпуск 040. Полный текст статей с кодом и таблицами.

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

Содержание Phrack 40

Автор: Dispater

P H R A C K 4 0

1 августа 1992 г.

~ Baby's Got Back! ~

Добро пожаловать в специальный юбилейный — сороковой — выпуск журнала Phrack! Прошёл почти месяц с тех пор, как мы кое-как оправились от феерии невероятно успешного SummerCon '92. Это была самая многочисленная тусовка за всю историю SummerCon; полный отчёт о событии можно найти в специальном материале за авторством Knight Lightning и меня самого — с помощью Holistic Hacker и Dr. Williams.

Brian Oblivion, чьё имя регулярно мелькает на страницах Phrack, возвращается со второй частью своего материала о сотовой телефонии (первая часть выходила в Phrack 38). Тематику телефонии в этом номере продолжает статья «Тонкое искусство телефонии» за авторством Crimson Flash — столь же глубокий и детальный материал, посвящённый RC/MAC, FACS и MARCH.

Невзирая на хвастовство надменных мерзавцев из Southwestern Bell и BT Tymnet относительно своей превосходной безопасности, похоже, они почти не причастны к выслеживанию и задержанию MOD в Нью-Йорке. Как уже знают некоторые из нас — MOD сдали свои же, из хакерского сообщества. Надо же, кто бы мог подумать.

Я не собираюсь играть в политику и выносить приговоры; лучше почитайте об этом в Phrack World News, часть 2, и сделайте выводы самостоятельно.

Раз уж мы заговорили о Tymnet, я счёл уместным <ухмыляется> включить в номер три статьи Toucan Jones на эту тему. Особый «воздушный поцелуй» — Dale Drew (он же The Dictator, он же Blind Faith, он же Bartman) за помощь и содействие в получении этой ценной информации. Неужели материал о TRW уже не за горами? Хм-м-м, может быть. :-)

Начиная с этого выпуска, Mind Mage будет помогать с Phrack Loopback в качестве нашего технического консультанта. Он будет отвечать на вопросы о технических проблемах — как для публикации, так и в частном порядке. Не стесняйтесь отправлять свои вопросы на phracksub@stormking.com — они будут переадресованы и получат ответ.

Раздел Loopback этого выпуска содержит очень важное сообщение от Jester Sluggo: он официально объявляет о своём уходе из хакерского сообщества. Sluggo вспоминает прошлое и даёт советы на будущее; я продолжаю преследовать так называемых профессионалов из антивирусного сообщества и разоблачать их истинные цели; а Sarlo проводит для нас экскурсию по Выставке потребительской электроники 1992 года в Чикаго — и это далеко не всё.

The Racketeer (Rack из The Hellfire Club) берёт бразды правления постоянной колонкой Network Miscellany, а Rambone возвращается с последними новостями о том, что происходит в подпольном мире торговцев компьютерным программным обеспечением — в рубрике Pirates Cove.

Taran King возвращается со специальным Phrack Pro-Phile, посвящённым Lex Luthor — основателю Legion of Doom и, пожалуй, самому легендарному хакеру андеграунда всех времён.

«Если это старше недели — у нас этого онлайн не найдёшь.»

Вас приглашают посетить отличную новую BBS под названием Planet 10. Если у вас есть хоть немного мозгов, вы, может быть, даже получите доступ. Planet 10 управляется Control C; сообщения и передачи файлов там настроены на удаление максимум через 1 неделю. Звоните по номеру (313)683-9722.

«Phrack — плохое влияние...»
-- TriZap, июль 1992 :-)

DISPATER, редактор Phrack
phracksub@stormking.com или phrack@well.sf.ca.us

```
                          We're Back and We're Phrack!

             "Phrack.  If you don't get it, you don't get it."

  "Whaddya mean I don't support the system?  I go to court when I have to!"
```

Реклама	AT&T, BellSouth и Секретная служба США
Творческий стимул	Camel Cool, Jolt Cola и Taco Bell
Шампунь	Mudge
Прочие помощники	Apollo, Brian Oblivion, Control C, Dr. Williams, Dokkalfar, The Gatsby, Gentry, Guido Sanchez, Holistic Hacker, Jester Sluggo, Legacy Irreverent, Lex Luthor, Mr. Bigg, Nihil, The Omega, The Pope, The Public, Sarlo, TriZap, Tuc, Voyager, White Knight

---

7	Тонкое искусство телефонии — Crimson Flash	65K
8	BT Tymnet, часть 1 из 3 — Toucan Jones	57K
9	BT Tymnet, часть 2 из 3 — Toucan Jones	55K
10	BT Tymnet, часть 3 из 3 — Toucan Jones	91K
11	SummerCon 1992 — Knight Lightning и Dispater	35K
12	PWN/Часть 1 — Datastream Cowboy	50K
13	PWN/Часть 2 — Datastream Cowboy	48K
14	PWN/Часть 3 — Datastream Cowboy	48K
	Итого:	702K

«Phrack. Журнал, который ТЕЛЕФОННАЯ КОМПАНИЯ не хочет, чтобы вы читали!»

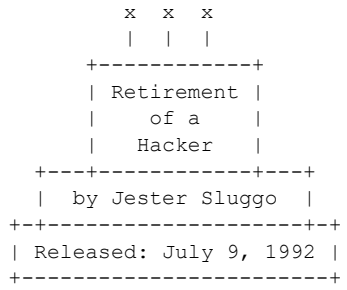
Phrack Loopback

Автор: Dispater & Mind Mage

Phrack Loopback — это форум для вас, читателей, где можно задавать вопросы, высказывать проблемы и обсуждать любые интересующие темы. Здесь же редакция Phrack публикует рецензии и рекомендации: журналы, программное обеспечение, каталоги, оборудование и прочее.

В этом выпуске:

• Уход на пенсию хакера — Jester Sluggo
• Правда вышла из моды — Dispater
• Вирус Тима Фоули — Guido Sanchez
• «Файлы хакера» (от DC Comics) — Newsbytes
• «Кроссовки» (от Universal Pictures) — пресс-релиз
• Пираты против AT&T: плакаты — Legacy Irreverent и Captain Picard
• Дайвинг в мусорниках телко приносит богатые плоды — Anonymous
• Анонимная почта в системах IBM VM? — Apollo
• Взлом WWIV Link — Mr. Bigg
• День гибели Bell System — Anonymous
• Выставка потребительской электроники 1992 года — Sarlo



Уход на пенсию хакера

Автор: Jester Sluggo
Опубликовано: 9 июля 1992 года

Я хотел бы начать с приветствия всем читателям этого текста, но, к сожалению, это будет последний раз. Более десяти лет я являюсь частью «хакерского подполья» и отношусь к редкому числу чрезвычайно везучих хакеров, которым удалось взломать немало компьютерных систем, телефонных сетей и других технологий, так и не попавшись. Я хочу воспользоваться этой последней возможностью, чтобы осмыслить пройденный путь и высказать ряд личных взглядов, — и хотя на сердце есть грусть, мне приятно объявить о своём официальном уходе из этого «подпольного» сообщества.

Решение уйти было тщательно спланировано несколько лет назад. В начале 1980-х взлом и исследование компьютерных систем ради жажды знаний было настоящим захватывающим приключением. Каждая система была словно неисследованная дверь, за которой открывались безграничные возможности: различные компьютеры, операционные системы, языки, сети, программы и данные.

Но уже во второй половине 1980-х я начал понимать, что должен направить свои интересы, знания и опыт в сторону легитимной карьеры. Зарабатывать на жизнь исключительно в рамках хакерского подполья практически невозможно, а идея использовать технологии ради денежной выгоды противоречит (негласному) кодексу хакерской этики. К тому же в это время осознание свободы исследования разных систем начало вытесняться пониманием реальной опасности: в столь молодом возрасте можно было загубить всё своё будущее, попавшись и получив судимость по законам США.

СМИ и правоохранительные органы почти всегда предвзято относились к хакерам — а это две весьма влиятельные силы, формирующие общественное мнение. Хакеров неизменно представляли в негативном свете, тогда как их открытия, усилия, изобретательность и упорный труд оставались незамеченными за пределами хакерской среды. В каком-то смысле это напоминает то, как правительство США и корпорации поддерживают научные исследования: группа учёных годами открывает, исследует, совершенствует или эксплуатирует определённую технологию, но их усилия остаются в тени, если результат не выливается в продукт, приемлемый для общества. Результаты исследований разделяются, оцениваются и оспариваются внутри научного сообщества задолго до того, как из них получится какой-либо продукт — если вообще получится. Точно так же, как учёные неустанно преследуют свои интересы, я искал ответы на свои вопросы и следовал своим увлечениям.

Именно те, кто стремится контролировать общество — правовая система и полиция, — навесили на «хакеров» ярлык злодеев. Хакеры умеют с помощью технологий получить доступ к самой разной информации, которая прежде была доступна лишь этим структурам, и эти стражи власти боятся потерять своё преимущество и контроль. Сейчас в США ФБР опасается утратить возможность легко прослушивать оптоволоконные линии и потому предлагает обязать телефонные узлы упростить им эту задачу. Если бы люди знали, как часто происходят незаконные прослушки, они были бы возмущены злоупотреблением властью. Полиция проводит незаконные обыски и аресты, а прокуроры подают неправомерные аффидавиты, чтобы сохранить контроль над информацией и доступом к ней.

Именно в середине и конце 1980-х годов правовая система и правоохранительные органы усилили давление, стремясь сурово карать хакеров, — и риск быть пойманным начал перевешивать азарт открытий. Нести бремя серьёзной уголовной судимости на протяжении всей жизни, когда тебе 20 лет (или того меньше — 16), невыносимо тяжело, как и вечный денежный долг, который влекут за собой такие последствия. В 1970-х основателей Apple застали за продажей Blue Box, когда те были студентами, и они отделались минимальным штрафом. По нынешним законам — с возможным тюремным сроком, денежными выплатами и гонорарами адвокатов — система могла бы загубить блестящие умы Стива Возняка и Стива Джобса. Быть может, компания Apple (и персональные компьютеры в целом) так и не появились бы на свет (IBM была бы в восторге).

Технологии меняются быстрее, чем успевают адаптироваться правовая система и общество, поэтому несанкционированное исследование этих технологий пока объявлено тяжким преступлением. Общество доверяет суждению законодателей, но даже в 1992 году они лишь начинают кое-как разбираться в технологиях: «Можно ли патентовать программное обеспечение (не путать с авторским правом), и в какой мере?», «Какая конфиденциальность и свобода слова должна быть у нас в электронной переписке и коммуникациях?» Не позволяйте некомпетентным законодателям принимать решения по технологическим вопросам, которые затронут вас, не зная вашей позиции.

Именно в конце 1980-х я начал готовиться к своему уходу. Я наметил цели и план их достижения. К сожалению, этот план требовал нескольких лет исполнения, но я понимал, что пришло правильное время для столь амбициозного начинания. Цели, которых я хотел достичь, были следующими:

1. Передать накопленные знания другим.

2. Поддержать активность хакерского движения.
3. Стать легитимно успешным, чтобы в качестве члена общества иметь возможность влиять на взгляды людей в отношении технологий.

Из-за растущей опасности быть пойманным и ради достижения успеха мне пришлось уйти в тень от основного хакерского сообщества и не афишировать свои действия. Первые две цели были тесно связаны между собой и заняли чуть больше времени, чем я изначально планировал. При этом они потребовали куда большей финансовой жертвы, чем я мог себе представить. Третья цель, вероятно, займёт всю оставшуюся жизнь, но это вызов, который я принимаю.

Чтобы выполнить цели 1 и 2, я провёл последние 5 лет, составляя «свод» информации и знаний, используемых в хакерском сообществе. Не всё в нём завершено, — но незавершено и зерно, из которого вырастает дерево. Любой, у кого есть телефон, может угадывать («взламывать», по версии СМИ и правоохранителей) четырёхзначные пин-коды телефонных карт или линий выхода PBX, — но мне нужны были «настоящие» хакеры. Я общался и встречался с сотнями хакеров по всему миру, чтобы найти тех, кто способен ответственно учиться и пополнять этот «свод» — людей, обладающих стремлением, уважением, трудолюбием и способностью вдохновлять новые поколения. Эта группа отобрана и обучена, и я считаю её одними из лучших кандидатов. Их международный состав должен открыть перед ними почти безграничные возможности и обеспечить определённую защиту. Желаю им удачи в бесконечном путешествии знания.

Стать легитимно успешным означало найти достойную работу. Очевидно, с моими интересами это должна была быть сфера высоких технологий. К сожалению, получить приглашение на собеседование или предложение о работе в таких компаниях крайне сложно: отделы кадров, как правило, отказываются нанимать хакеров. Это иронично, ведь многие инженеры и программисты в этих же компаниях — сами бывшие хакеры или люди со схожим страстным интересом к технологиям. К тому же лучший опыт хакера получен нелегитимным путём и не может быть указан в резюме.

Первым шагом к этой цели стало инстинктивное решение: сохранить искренний азарт и увлечённость технологиями. Звучит странно, но многие хакеры знают друзей, которые «выгорают» от хакерства или работы в высокотехнологичных компаниях, — и я не хотел выгореть в 20 лет, поэтому пришлось притормозить свою хакерскую активность.

Следующим шагом стало высшее образование, которое я и получил. Университет — не ответ на все вопросы... собственно, ни на какие вопросы он не отвечает, однако это опыт, который я желаю каждому, — уникальный опыт. Диплом не гарантирует работу, но может помочь пройти через отдел кадров. Если есть возможность поступить в университет — не упускайте её. Я понимаю, что работодатели предпочитают опытных специалистов «свежим» выпускникам, но если у вас есть сосредоточенный интерес к определённой технологии, вы найдёте способ постоянно развиваться, даже страдая сквозь годы учёбы. И как это вышло у меня: диплом в сочетании с результатами целенаправленных усилий откроет вам лучшие карьерные возможности. Будьте сосредоточены и терпеливы... у меня сработало!

Сейчас я работаю внутри технологической компании и получаю удовольствие от своего дела. Порой я даже думаю про себя: «Неужели мне за это ещё и платят?!» Это восхитительно — делать то, что делаю я, — однако нужно много работать и продолжать работать, чтобы подняться как можно выше и максимально реализовать свои способности. Делая это, я надеюсь когда-нибудь отдать что-то обществу — не хакерскому, — что покажет людям: хакеры полезны для общества и способны изменить укоренившийся негативный образ, уравнявший хакеров с «преступниками». Я хотел бы видеть зрелых, легитимно успешных хакеров, объединённых в группу по интересам для поддержки энергии молодых хакеров.

Хотя я ухожу из сообщества, я не могу уйти от любопытства и неистового интереса к технологиям. Теперь я направляю их в законное русло — в повседневную работу — и намерен делать это

впредь. Я безмерно наслаждался участием в хакерском сообществе и всегда буду это ценить. Я также надеюсь в конце концов убедить людей принять хакеров и прекратить их преследовать. Эта последняя цель — самая амбициозная, но я считаю её важнейшей: те, кто управляет обществом, растрачивают впустую группу молодых и талантливых людей, способных стать изобретателями технологий будущего. И вот теперь я официально говорю «прощай» своим друзьям в хакерском сообществе... но не в последний раз.

Не сдавайтесь,
Jester Sluggo

«Правда вышла из моды»

Подзаголовок: Расследовательский репортаж о коррупции в сфере компьютерной безопасности

Автор: Dispater

Похоже, в наши дни антивирусная индустрия/сообщество промыло мозги публике, убедив её, что любое использование модема немедленно подвергает пользователя немыслимому множеству опасностей. Звучит примерно как слова мамы, когда она не хотела отпускать вас гулять после темноты — правда?

Как выяснилось, антивирусное сообщество нравственно не отличается от телевизионных проповедников. Пока они вещают об ужасах доступа к информации (без покупки одного из их продуктов), сами занимаются именно тем, что, по их словам, следует сделать федеральным преступлением на уровне Конгресса. А именно — «распространением компьютерных вирусов». Мало того, что они занимались этим с самого начала существования индустрии, так теперь внутри неё появилась самозваная «элита» [ухмылка] так называемых профессионалов, которые стремятся сохранить монополию на торговлю вирусами, уничтожая репутацию и жизни независимых исследователей. Фактически в сфере компьютерной безопасности возник своего рода «вирусный картель».

The Little Black Book of Computer Viruses

The Little Black Book of Computer Viruses — печатный текст, появившийся несколько лет назад, который наконец привлёк внимание людей, считающих Prodigy и CompuServe лучшими сетями в мире. Книга содержит исходные тексты вирусов. Надо же, как сложно людям добраться до вирусов, правда? Ну что ж, один информационный динозавр снискал себе известность, публично осудив подобную «безнравственность».

> *«Профессиональные борцы с вирусами, такие как Алан Соломон из S&S International, злятся, как потревоженные шершни, из-за этой публикации. Они организуют антикнижные кампании, включающие ПИКЕТ У ДОМА АВТОРА, бойкот магазинов, продающих книгу, петиции в Конгресс и даже привлечение адвокатов.»*
> *— ComputerWorld, 29 июня 1992 года, стр. 4 (выделено нами)*

Примечательно, что пока мистер Соломон поощряет личные и экономические преследования мистера Людвига, его близкая подруга и деловой партнёр Сара Гордон выполняет за него грязную работу.

Конференция

1-я ежегодная конференция Национальной ассоциации компьютерной безопасности (NCSA) по вирусам прошла в Вашингтоне, округ Колумбия, в июне прошлого года. Алан Соломон и Сара Гордон присутствовали в полном составе. Гордон нередко называют верной помощницей Соломона, и нигде она не оправдала этот титул так ярко, как на этой конференции.

Там Гордон купила не одну, а две копии книги Людвига, а затем немедленно бросилась к организатору конференции, чтобы устроить театральную сцену о том, какой аморальностью является продажа подобного. Как выясняется, это не первый случай, когда Сара Гордон прибегает к столь лицемерному поведению.

Ещё одна примечательная деталь конференции: однажды вечером Knight Lightning и несколько его товарищей заметили людей, собравшихся в одной из комнат, и из любопытства заглянули. Оказалось, это была своего рода «полночная встреча». KL и его друзей попросили уйти, поскольку «им здесь не место». Почему? Потому что собравшиеся обсуждали способы «положить конец» ряду BBS и нанести вред карьерам людей, распространяющих вирусы.

Некоторое время спустя после конференции мне стало известно об их плане «использовать СМИ для разрушения репутации этих сисопов. Например, воздействовать на прессу, чтобы привлечь внимание к подобной деятельности». Эти люди даже составили список BBS, которые они намерены «закрыть» в первую очередь.

Список целей

Phrack получил анонимное письмо с «чёрным списком» BBS, составленным этой самозваной «элитой» сетевых линчевателей. После его получения редакция Phrack связалась с сисопами перечисленных систем, и в результате многие номера с тех пор изменились.

```
+1-206-481-2728  The Festering Pit of Vile Excretions
                 [Этот телефон принадлежит строительной компании
                 Custom Building Co.]
+1-213-274-1333  West Coast Technologies (Tymnet 311021300023)
+1-213-274-2222  DII
+1-213-PRI-VATE\
                )BBS-A-Holic
+1-ITS-PRI-VATE/
+1-301-PRI-VATE\
                )Digital Underground
+1-301-913-5915/
+1-301-948-7761  Cornerstone III
                 [              ]
+1-305-669-1347  The Penthouse
+1-516-466-4620\
                )Hamburger Heaven: была недоступна из-за проблем с ПО,
+1-517-PRI-VATE/ прежде называлась Sentinel's Gate
+1-602-491-0703  The Final Frontier
+1-708-541-1069  Pirate's Guild
+1-717-367-3501  Night Eyes
+1-818-831-3189  Pirate's Cove
+1-901-756-4756  Silicon Central
+1-916-729-2112  The Welfare Department
                 [Это телефон страховой компании]
+1-213-274-1333  West Coast Technologies (Tymnet 311021300023)
+1-213-274-aaaa  DII
+1-313-LIM-ITED  Canterbury Woods
+1-409-372-5511  The Crowbar Hotel
+1-514-PRI-VATE\
                )The Sacred Reich
+1-514-975-9362/
+1-516-328-0847  The Grave of the Lost
+1-516-541-6324  Realm of Heroes
+1-708-459-7267  Hell Pit
+1-713-464-9013  South of Heaven
+1-818-831-3189  Pirate's Cove
```

```
+1-819-PRI-VATE  Brain Damage
```

Кто именно стоит за организацией этой группы и кто составил и распространил список — неизвестно, однако среди участников были представители CERT, ISPNews, а также ряд известных лиц, именующих себя экспертами по безопасности, и толпа безвестных личностей, желающих сделать себе имя.

Hell Pit BBS

Hell Pit — это BBS в Чикаго под управлением сисопа по имени Kato. У Kato есть законный (как будто любопытство нуждается в оправдании) интерес к устройству вирусов. Предоставим ему слово:

> *«Я управляю The Hell Pit BBS уже три года. За это время система прошла через разные этапы, но в последнее время главным моим увлечением стали компьютерные вирусы. Я заинтересовался ими примерно полтора года назад и создал на своём сервере файловую базу с вирусами. Поначалу у меня было всего 5–6 вирусов, собранных с одной местной системы. Сейчас коллекция выросла примерно до 700 вирусов для IBM-совместимых компьютеров.»*
>
> *«Похоже, их цель — закрыть мою BBS и тем самым уничтожить мою базу вирусов. Учитывая, что эти антивирусные деятели заявляют о своей заинтересованности в вопросах компьютерной безопасности, их тактику я нахожу весьма сомнительной. Недавно прошла антивирусная конференция NCSA. Из источников мне стало известно, что один из участников конференции [Сара Гордон] совершил определённые действия на моей BBS. По словам этого человека, он позвонил, загрузил 3 поддельных вируса, получил доступ к моей базе и скачал несколько вирусов. Это они называют доказательством того, что я недостаточно контролирую доступ к вирусам на своей системе. Антивирусное сообщество не даёт мне возможности защититься.»*
>
> *«Сами антивирусные специалисты совершали те же ошибки, что и я, — пожалуй, куда чаще. Никакого чёткого набора правил, определяющих, кто является антивирусным авторитетом, не существует. Некоторые люди, соответствующие негласным критериям, могут обмениваться вирусами с антивирусным сообществом. Каковы эти критерии? Есть ли они вообще? По моему опыту, если ты вращаешься в нужных кругах — тебя признают антивирусным авторитетом. Однако в антивирусном сообществе немало путей, по которым вирусы могут утечь наружу. Ведь никогда нельзя быть уверен, с кем имеешь дело. То, что человек умён и заявляет об антивирусных убеждениях, вовсе не означает, что он не пишет вирусы втайне.»*
>
> *«На антивирусных конференциях вроде конференции NCSA участники обменивались вирусами, как бейсбольными карточками. Это я не назову контролем над доступом.»*
>
> *«Они действительно помогают многим людям с компьютерными проблемами. Однако критиковать меня за ненадлежащий контроль доступа к моей коллекции вирусов — лицемерие.»*
>
> *«Если кто-то хочет проверить мою систему лично — милости прошу. У меня есть много чего кроме вирусов: хорошая подборка текстовых файлов и весьма активные форумы. The Hell Pit BBS — (708)459-7267.» — Kato*

Выводы

Похоже, в антивирусном сообществе зреет движение, цель которого — избавить мир от BBS, открыто и свободно распространяющих вирусы. Антивирусные профессионалы считают, что

обязаны «защищать мир» от подобной деятельности. При этом на недавней конференции в Вашингтоне стало известно, что один из антивирусных исследователей лично загрузил три вируса на вирусную BBS (Hell Pit). Зачем? Чтобы «разоблачить то, что сисоп не столь осторожен, как утверждает». После этого тот же человек смог скачать вирусы, нарушив тем самым правила, о которых заявлял сисоп (впрочем, это утверждение основано на честности самого антивирусного сообщества — а она, как очевидно, весьма сомнительна).

Таким образом, антивирусное сообщество подставило сисопа, сделало из него показательный пример на национальной конференции — не дав ему ни малейшей возможности защититься. Возможно, сисоп до сих пор ничего об этом не знает — вплоть до сего момента.

Те же антивирусные исследователи открыто обменивались копиями вирусов «исключительно в исследовательских целях». Им, значит, можно распространять вирусы во имя науки — благодаря их самопровозглашённой важности в антивирусном сообществе, — а тех, кто угрожает их элитному (НЕТ!) статусу, следует подставлять и делать из них пример для устрашения.

Делай, как я говорю, а не как я делаю

Всё это порождает очень важный вопрос: кто дал частным специалистам по компьютерной безопасности или консультантам карт-бланш на подобную деятельность? Особенно когда они при этом имеют наглость навешивать на хакеров ярлык преступников за то же самое. Ответ — не кто, а что: деньги и самолюбие. Пожалуй, самым пугающим аспектом всей этой ситуации является то, что настоящая битва здесь ведётся не вокруг вирусов и BBS, а вокруг свободного распространения информации. Для группы людей, столь глубоко погружённых в эту сферу, поразительно полное непонимание концепции прав Первой поправки.

Phrack Magazine готов стоять твёрдо и неустанно следить за любым посягательством на эти права и защищать их. Мы работаем давно, нам известно, где зарыты тела, наши многочисленные последователи и читатели держат глаза и уши открытыми по всей стране. Предупреждаем всех в сфере безопасности: стоит вам оступиться — мы будем рядом, чтобы вас разоблачить.

Dispater

Вирус Тима Фоули

Автор: Guido Sanchez

Вскоре после того, как я переехал из зоны 512 в 708, мне не повезло осознать: Steve Jackson Games — компания, чьи игры я охотно покупаю и в которые играю, — держала BBS в моём родном городе под названием Illuminati BBS. Не повезло потому, что в Техасе я мог звонить туда по местному тарифу, а теперь приходилось оплачивать этот звонок из Иллинойса.

Примерно через год после налёта Секретной службы на Steve Jackson Games, когда большинство «улик» вернули с маленькими зелёными наклейками, на BBS был выложен текстовый файл FOLEY.TXT — простая копия иска, поданного Steve Jackson Games против правительства, известного также как JACKSUIT.TXT, распространённого, насколько я понимаю, организацией EFF.

[Примечание редакции: нам не удалось подтвердить, что EFF когда-либо распространяла файл с именем JACKSUIT.TXT; однако подробности участия EFF в судебном процессе Steve Jackson Games можно найти в EFFector Online 1.04.]

Файл назывался FOLEY.TXT, очевидно, из-за Тимоти Фоули — большой шишки от правительства [на самом деле агента Секретной службы США], одного из ответчиков по делу. Я скачал файл и

запаковал его в архив, который, что неудивительно, назвал FOLEY.ZIP.

В течение следующей недели я, как обычно, радостно распространял информацию и загрузил FOLEY.ZIP вместе с партией вирусных файлов на местную BBS с только что созданной базой вирусов. Идея состояла в том, чтобы распространять вирусы повсюду, делая их доступными всем, — чтобы замечательные маленькие авторы антивирусов не могли преуспеть.

К сожалению, FOLEY.ZIP попал в вирусную базу, и прежде чем я успел предупредить сисопа о необходимости переместить его в нужную категорию, примерно 8 недотёп-варезников уже скачали файл — к концу недели он разошёлся по всей зоне NPA 708.

Мораль этой истории? Никакой, в общем-то. Это просто забавная зарисовка о том, что может произойти, когда люди окунаются в интенсивный бартер информации через модем: можно стать посмешищем, если не уверен в том, что именно ты распространяешь. Вот и весь этот огромный бизнес: каждый — курьер. Будь то пиратские файлы, файлы для взрослых, звуковые файлы, вирусы или текстовые документы — в 90% случаев их просто скачивают с одной 1,2-гигабайтной борды и загружают на следующую, чтобы получить кредиты и скачать ещё, и так по кругу.

Большой замкнутый цикл — совсем как жизнь. Рискуя показаться банальным, призываю всех: «Притормозите! Откиньтесь назад, сорвите розы, съешьте их, переварите и в итоге выделите их!» Мистер Уорхол, мои пятнадцать минут истекли. Трибуна свободна.

---

22 июня 1992 года

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

НЬЮ-ЙОРК — Компания DC Comics объявила о выходе нового серийного комикса из двенадцати выпусков — «Файлы хакера» (*The Hacker Files*). Представитель DC Марта Томасес сообщила, что первый выпуск поступит в продажу 23 июня.

Серия создана писателем-фантастом Льюисом Шайнером и рассказывает о приключениях «суперхакера» Джека Маршалла, который до начала описываемых событий несправедливо лишился работы в компании Digitronix и теперь работает независимым консультантом.

Первая сюжетная линия, охватывающая первые четыре выпуска, посвящена попытке Маршалла выяснить, кто несёт ответственность за блокировку ARPANET (сети Агентства перспективных исследований) и вызванные неполадки в Центре космического наблюдения NORAD в Шайенн-Маунтин, штат Вайоминг, едва не поставившие США на грань ядерной войны.

В ходе расследования Маршаллу, известному под псевдонимом «Хакер», помогает ряд членов хакерского сообщества: «Master Blaster», «Sue Denim» и «Spider» (Master Blaster, настоящее имя — Майки, — учится в Бронксской специализированной школе естественных наук в Нью-Йорке).

Вымысел сближается с реальностью, когда выясняется, что за вирусом, причинившим все разрушения, стоит Роджер П. Сильвестр — студент Колумбийского университета и сын высокопоставленного сотрудника Агентства национальной безопасности (АНБ). Параллель очевидна: 2 ноября 1988 года Роберт Т. Моррис-мл., студент Корнелльского университета и сын главного специалиста АНБ по компьютерной безопасности, парализовал Интернет, запустив «Интернет-червь».

Шайнер рассказал Newsbytes: «Сходство персонажей, разумеется, намеренное — можно даже заметить довольно тонкую игру имён: "Sylvester The Cat" и "Morris The Cat". Я сделал это отчасти для того, чтобы читатели, хоть немного разбирающиеся в компьютерах, поняли: сюжет не взят из воздуха, а стал результатом серьёзного исследования».

Шайнер продолжил: «Читая комиксы, я ищу насыщенность информацией, и постарался сделать "Файлы хакера" богатыми именно в этом отношении. Я надеюсь привлечь к комиксам технически

грамотную молодёжь — комиксы были одним из первых медиа, широко использовавших компьютеры, и с помощью "Файлов хакера" я хочу вовлечь в этот жанр больше людей, увлечённых технологиями».

Шайнер также сообщил Newsbytes, что опыт программиста в небольшой далласской программной фирме поддерживал его постоянный интерес к компьютерам и телекоммуникациям. Он добавил: «Фирму купила EDS (Electronic Data Services), компания Росса Перо, — а с моими длинными волосами и джинсами я не вписывался в корпоративный стиль EDS, так что ушёл и сосредоточился на писательстве».

«Кроссовки» — Universal Pictures

24 июня 1992 года

Взято из PR Newswire

Следуйте за командой высокотехнологичных экспертов по безопасности в сложный мир компьютерных преступлений

> *«Я пытался взломать Protovision. Хотел заполучить программы для их новых игр.» — Дэвид Лайтман (Мэттью Бродерик, «Военные игры»).*
>
> *«Мир больше не управляется оружием, энергией или деньгами. Он управляется маленькими единичками и нулями. Маленькими битами данных. Это всего лишь электроны.» — Космо (Бен Кингсли, «Кроссовки»).*

В 1984 году сценаристы Уолтер Ф. Пэркс и Лоренс Ласкер были номинированы на премию Академии за сценарий о приключениях молодого школьного хакера (Мэттью Бродерик), чей компьютер вышел на связь с мэйнфреймами Командования воздушно-космической обороны Северной Америки (NORAD).

«Военные игры» — кассовый и критический успех — стали первым крупным голливудским фильмом, исследующим нарождающийся мир компьютерных игр, взломов, крахов систем и пиратства данных. Картина быстро обрела армию поклонников среди тех, кто тоже открыл для себя необъятные горизонты персонального компьютера.

Восемь лет спустя Пэркс и Ласкер вместе со сценаристом-режиссёром Филом Алденом Робинсоном («Поле чудес») работают над «Кроссовками» — выпуском Universal Pictures, прослеживающим путь команды высокотехнологичных экспертов по безопасности в сложном мире компьютерных преступлений. В авантюрном фильме режиссёра Робинсона снялись Роберт Редфорд, Дэн Эйкройд, Бен Кингсли, Ривер Феникс, Сидни Пуатье, Дэвид Стрэтэйрн, Джеймс Эрл Джонс и Мэри Макдоннелл.

Слово «кроссовки» Пэркс и Ласкер впервые услышали на компьютерной конференции в 1981 году — как прозвище юных программистов IBM. Несколькими месяцами позже они встретили редактора небольшого компьютерного журнала, который дал этому слову совсем иное определение. «Кроссовки», объяснил их источник, — это синоним понятий «чёрные шляпы» и «тигровые команды», то есть люди, которых нанимают для взлома систем с целью проверки безопасности объектов.

Объединившись с Робинсоном, трио набросало основной сюжет о команде «кроссовок», которых тёмное прошлое свело вместе. Затем Робинсон приступил к масштабному исследованию: то, что начиналось как сбор базовых фактов о компьютерных нарушителях, вскоре переросло в тайные встречи с хакерами из подполья, агентами ФБР, криптологами, специалистами по прослушке,

профессиональными взломщиками и нескончаемым потоком киберпанков — пионеров проникновения в системы.

В процессе исследования «Кроссовок» состоялись встречи с самыми разными персонажами — от печально известного Captain Crunch (Джона Дрейпера) до выдающегося математика Леонарда Адлемана, которого называют отцом криптографии с открытым ключом. Используя компьютерное шифрование как сюжетный приём, авторы создали замысловатую историю в жанре «а что, если», исследующую возможность существования «чёрного ящика», способного потенциально взломать любую электронную информацию в мире.

«"Кроссовки" — это про новую эпоху... информационную эпоху», — сказал Редфорд. «Вполне возможно, что война будущего — это война за информацию. Кто ею владеет — побеждает».

Выход в кинотеатрах — этот сентябрь.

Пираты против AT&T;: плакаты

Особая благодарность Legacy Irreverent и Captain Picard

24 мая 1992 года двое одиночек-пиратов — Legacy (из CyberPunk System) и Captain Picard (из Holodeck) — наконец решили, что с них хватит AT&T. Вместе они отправились к Техническому центру обслуживания AT&T (к западу от Годдарда, штат Канзас) и объявили это место собственностью пиратов и хакеров повсюду.

Они водрузили флаг «Весёлый Роджер» с черепом и костями на флагштоке AT&T, где он и оставался двое суток, пока служба безопасности его не сняла.

Это событие было заснято на фото и видео студией EGATOBAS Productions, чтобы сохранить этот исторический момент. Теперь вы можете увидеть его своими глазами. В течение ограниченного времени они предлагают полноцветные постеры и футболки с изображением пиратского «Весёлого Роджера», гордо развевающегося над AT&T с логотипом компании на видном месте и подписью: «МЫ ПРИШЛИ, МЫ УВИДЕЛИ, МЫ ПОБЕДИЛИ».

```
Цены:  Полноцветный постер 11" x 17"..................... $ 7.00 US
       Полноцветный постер 20" x 30"              $20.00 US
       Футболки                                   $20.00 US
```

Для заказа отправьте чек или денежный перевод на сумму плюс $1.00 US за доставку по адресу:

```
CyberPunk System
P.O. Box 771027
Wichita, KS  67277-1072
```

Для футболок обязательно укажите размер.

GIF-изображение также доступно через CyberPunk System, 1:291/19, 23:316/0, 72:708/316, 69:2316/0. FREQ magicname PIRATE

Дайвинг в мусорниках телко приносит богатые плоды

20 июля 1992 года

Автор: Anonymous

Несколько дней назад передо мной встал выбор: как провести чудесный вечер — помириться с подругой или порыться в мусоре у здания Bell Central Office. Видимо, я настоящий неудачник, раз выбрал телко, — но моя страсть не осталась без награды: мне попалась отличная находка.

Здание — старая кирпичная постройка 1940-х годов практически без охраны: в воскресенье вечером там даже охранника не было. Так что проблемой не стало перелезть через колючую проволоку вокруг грузовой площадки, где и стоял мусорный контейнер. Покопавшись в нём в поисках чего-нибудь стоящего, я наткнулся на коробку среднего размера, явно служившую кому-то из сотрудников для переезда: на ней было написано «кастрюли и сковородки, кухня».

Заинтригованный странной коробкой в мусоре телко, я открыл её — и был немало удивлён! На меня смотрел скоросшиватель с наклейкой «Phrack 23». Внутри оказалась полная коллекция Phrack 1–39, Informatik 1–4, а также LOD/H Technical Journals 1 и 2 (похоже, на большее у них не хватило денег на печать). Напечатано было небрежно на лазерном принтере (или аккуратно на струйном), но всё равно куда лучше, чем моя собственная распечатка. :-)

Судя по всему, кто-то в телко — фрикер, пробравшийся в ряды South Central Bell, или там просто следят за последними новинками в сообществе фрикеров и хакеров.

Может, это и не столь ценно, как список паролей COSMOS или номера дозвона, — но находка всё равно знатная.

Анонимная почта в системах IBM VM?

```
Дата: Вт, 28 апр 92, 14:54:58 EST
От: Apollo
Тема: Анонимная почта
Кому: Редакция Phrack
```

Уважаемая редакция Phrack,

Читая один из прошлых номеров Phrack, я заметил, что анонимную почту можно отправлять с UNIX-системы. Я знаю, что есть способ сделать это и с VM-системы. Однако администраторы моего узла не хотят, чтобы анонимная почта отправлялась, поэтому и не говорят, как это делается. Не мог бы кто-нибудь рассказать мне, как отправить анонимную почту через VM-систему?

— Apollo —

```
От: Mind Mage
Тема: Анонимная почта
Кому: Apollo
```

Полагаю, вы знаете, что можно подключиться по telnet к любой VM-системе в Интернете и отправить анонимную почту через порт 25 с командами, весьма похожими на UNIX SMTP.

Если вы хотите сделать это со своей конкретной системы, попробуйте подключиться по telnet к порту 25 своей же машины и отправить письмо оттуда.

Mind Mage

Взлом WWIV Link

Автор: Mr. Bigg (Rebel-*-Jedi)

Мало кому это интересно, но вот небольшой трюк, на который я случайно наткнулся и хочу поделиться.

Взлом систем WWIV с использованием мода Multi-Net v1.0
Обычно применяется для LinkNet

```
Main Login: @-!NETWORK!-@
Link Login: 1 (или кто там является сисопом)
//edit config.dat
найти системный пароль в файле
прервать редактирование
//dos
ввести системный пароль
```

Вуаля — доступ к DOS. :)

Забавно, что пароля там нет вовсе. Перед использованием этого мода проверяйте список пользователей.

День гибели Bell System

На мотив «American Pie» (с извинениями перед Доном Маклином)

```
Давным-давно,
Я всё ещё помню,
Когда местные звонки были «бесплатными».
И я знал: плачу по счетам,
Не желаю им зла —
И телефонная компания оставит меня в покое...

Но дядюшка Сэм решил, что знает лучше,
Раздробил их навсегда!
Мы дадим простор конкуренции:
Это добрый капитализм!

Не помню, плакал ли я,
Когда мой счёт впервые вырос втрое.
Но что-то задело меня в самую душу
В день... гибели... Bell System.

И мы пели...

Прощай, Ма Bell, зачем ты умерла?
Шипение Sprint и эхо MCI,
«Местные звонки нас разорили!» — кричим мы все.
О Ма Bell, зачем ты должна была умереть?
Ма Bell, зачем ты должна была умереть?

В твоём офисе — Step by Step,
Или уже добрался Crossbar?
Все когда-то спрашивали...
О, скоро ли придёт TSPS?
IDDD будет благом!
И я надеюсь получить тоновый телефон уже скоро...

Цветные аппараты — это здорово,
И прямой набор вне конкуренции!
Мой код зоны — «низкий»:
Признак престижа!

Ах, они только что подняли цену в будках до десяти центов!
Что ж, видимо, пора.
Помню, как звенели монеты в таксофонах
В день... гибели... Bell System.
И мы пели...
```

Прощай, Ma Bell, зачем ты умерла?
Шипение Sprint и эхо MCI,
«Местные звонки нас разорили!» — кричим мы все.
О Ma Bell, зачем ты должна была умереть?
Ma Bell, зачем ты должна была умереть?

Тогда у нас был единый тариф,
Установка телефона не вызывала споров
О том, кто куда тянет провод...
Монтёры приезжали прямо к тебе,
Никаких «телефонных магазинов» с их шумихой,
И 411 был бесплатным — казалось справедливым!

Но ФКС, похоже, задумала
Позволить другим снимать сливки дальней связи,
Наплевав на местные линии —
Ведь там живут одни деревенщины!

И вот однажды случилось то,
Чему суждено было случиться:
Великая Bell System рухнула.
В её обломках мы собираемся все вместе,
В день... гибели... Bell System.

Прощай, Ma Bell, зачем ты умерла?
Шипение Sprint и эхо MCI,
«Местные звонки нас разорили!» — кричим мы все.
О Ma Bell, зачем ты должна была умереть?
Ma Bell, зачем ты должна была умереть?

Я приехал в Мюррей-Хилл,
Чтобы навестить Bell Labs, скоротать время,
Но вывеска гласила: Labs уже нет.
Я вернулся к своему старому CO,
Где раньше были мои телефонные линии,
Но там было пусто, темно и так уныло...

Реле не стучали,
Данные не пели,
Тональные сигналы MF замолкли,
Ни слова больше не было сказано,
Все несущие каналы оборваны...

И вот как это всё случилось,
Рупоры микроволновых антенн стали гнёздами птиц,
Всё стало таким абсурдным,
В день... гибели... Bell System.

Прощай, Ma Bell, зачем ты умерла?
Шипение Sprint и эхо MCI,
«Местные звонки нас разорили!» — кричим мы все.
О Ma Bell, зачем ты должна была умереть?
Ma Bell, зачем ты должна была умереть?

Мы пели:

Прощай, Ma Bell, зачем ты умерла?
Шипение Sprint и эхо MCI,
«Местные звонки нас разорили!» — кричим мы все.
О Ma Bell, зачем ты должна была умереть?

Выставка потребительской электроники 1992 года

Автор: Sarlo

Выставка потребительской электроники — ежегодное мероприятие в Чикаго, штат Иллинойс, дающее возможность заглянуть в будущее электронных товаров, а также познакомиться с тем, что уже есть на рынке.

Как правило, выставка закрыта для широкой публики. Однако в этом году за скромные 10 долларов любой желающий мог преспокойно явиться к воротам, получить зелёную штампик на руку и осматривать экспонаты, охая и ахая, разинув рот перед стендами таких компаний, как AT&T, большинство крупных телефонных компаний Bell, IBM, Prodigy, десятки производителей сотовых телефонов, Nintendo, Sega и больше производителей программного обеспечения, чем у меня хватит терпения перечислять.

Я беру такси до Конгресс-центра Маккормика — настоящей выставочной Мекки — и вхожу через подземный вход. Иду по ничем не примечательному коридору, отмечая, что для центра, который должен демонстрировать новейшие технологии будущего, ничего особо захватывающего здесь нет. В ожидании унылого шоу с посредственной видеографикой покупаю билет, ставлю штамп на руку и вхожу.

Огромный зал обрушивается на органы чувств светом и звуком. Кажется, в воздухе пахнет кремнием, пока я иду по проходу мимо гигантского экрана Phillips Digital Compact Cassettes. Не будучи большим фанатом аудиооборудования, направляюсь к стенду Sharp Electronics. Это оказывается шагом в правильном направлении: я оказываюсь лицом к лицу с одним из самых чётких и, судя по названию, самых «острых» видеодисплеев в своей жизни. ЖК-телевизоры с большим экраном демонстрируют сцену с аквариумом. Даже вблизи искажений почти нет. Вдоль северной стены выставлена уменьшенная версия ЖК-дисплея в разрезе — любители электроники могут изучить внутреннее устройство экрана. Свернув за угол, я оказываюсь перед их двухпроекционным настенным телевизором. Никаких двойных изображений и размытой картинки — по моим ощущениям, это лучшая система видеопроекции, с которой мне доводилось сталкиваться.

Сотовое безумие

Гвоздём раздела сотовых телефонов стала экспозиция Motorola Cordless/Cellular с большим плакатом, изображающим корпоративного представителя Motorola. Над ним броский слоган:

> ***«Подслушиватели радиотелефонов — везде.»***

Немедленно заинтересовавшись, подхожу, чтобы прочитать текст помельче:

> *«Но с моим радиотелефоном Motorola Secure Clear™ мои личные разговоры остаются личными.»*

Secure Clear, как объясняет рекламный материал, — это эксклюзивная технология, гарантирующая, что ни один подслушиватель не сможет воспользоваться другим радиотелефоном, сканером или радионяней, чтобы прослушать ваши переговоры.

Как большинство из нас знает, коды безопасности и многоканальность не всегда защищают от прослушки. Благодаря новейшим технологиям, коды безопасности — один из 65 000 возможных, случайно присваиваемых каждый раз при установке трубки в базу, — не позволяют чужим использовать вашу базу в качестве исходящей линии.

С помощью функции Auto Channel Scan (ACS) радиотелефоны Secure Clear автоматически пропускают каналы с шумом или помехами. Гадать, что Sarlo попросит на Рождество, не придётся.

Для получения дополнительной информации о Motorola звоните в их отдел потребительских товаров: (800)331-6456.

Среди прочего, компания Technophone представила широкий спектр аксессуаров для сотовых телефонов: настольную подставку, запасные аккумуляторы, автомобильное зарядное устройство,

новую линейку антенн, быстрые AC-зарядники QuickCharge и гарнитуру для безопасного использования в автомобиле.

Компания Omni Cellular выставила открытую для демонстрации модель портативного телефона «A» V833k, позволив всем желающим провести разговор с сотрудником без помех. Среди характеристик:

• 90 минут разговора
• 10 часов в режиме ожидания
• Прочная конструкция, собранная в США

Дополнительные функции: автоматическое отключение питания, электронная блокировка, память на 50 номеров, индикатор уровня сигнала.

Веселье в восточном корпусе

Начав скучать, подхожу к карте. Ищу — и нахожу, почти буквально, свой зелёный свет. На подсвеченной карте выставки зелёный сектор словно манит меня к себе.

«Компьютеры»

Мчусь к двери, на секунду задерживаясь для проверки сумок охранником, и врываюсь в восточный корпус (по дороге купив крутую футболку CES-92) с новым порывом.

Прямо у входа бьёт в нос запах людей в деловых костюмах и дешёвых компьютерных услуг. Мигом понимаю: вот он — стенд Prodigy.

Сотрудники раздают пробные подписки и агитируют потребителей подписаться на их сервис. Решаю взглянуть.

«Где ещё вы найдёте такой замечательный сервис с доступом к такому широкому кругу вещей, как онлайн-сообщения, актуальные новости, онлайн-энциклопедия и тысячи интересных пользователей, таких же, как вы?» — расхваливает товар сетевой зазывала, не просто вводя потребителей в заблуждение насчёт полезности Prodigy, но ещё и с немалой наглостью суя им под нос PS/1, именуя его качественным компьютером.

«Хм... а как насчёт любого публичного Unix-сервера с доступом к Интернету или Usenet?» — спрашиваю я. Самодовольный тип встаёт на котурны.

«Возможно. Но большинство публичных Unix-систем и BBS не имеют качественной графики, дополняющей информацию». Мужик, очевидно, изучил тему. Но судя по всему, IBM и Sears так основательно промыли ему мозги, что он и сам поверил в ту чушь, которую впаривает людям.

«Да», — говорю я. «Но большинство публичных серверов не тратят четверть экранного места на бесполезную рекламу. И я не осознавал, что красивые картинки делают новости или сообщения информативнее. Также позволю себе заметить: они не берут с вас дополнительных денег за каждое сообщение сверх тридцатого, не читают вашу почту и не цензурируют публичные посты, и зачастую вообще не берут никакой платы — разве что необязательную подписку, максимум долларов 50 в ГОД, — и не хранят маленькие файлы данных, собирающие информацию о подписчиках из жировой таблицы». Пока я говорил, продавец пытался меня прервать и в этот момент ему наконец удалось.

«Ну, вижу, у вас много вопросов», — ловко уходит продавец. «Уверен, вот этот джентльмен с удовольствием ответит на них, а я пока отвечу на вопрос этой дамы... Да?»

Ко мне подходит другой сотрудник, интересуясь, какие у меня вопросы. Говорю, что никаких — меня эта система не особо интересует, просто хотел посмотреть, как продавцы Prodigy держатся под давлением. Он отвечает, что охотно ответит на любые мои вопросы, но если я здесь только

чтобы мешать работе, лучше мне уйти.

Дальше — по другим стендам. Здесь бесплатно раздавали журналы, в том числе Mobile Office, разные журналы о Nintendo и игровых системах, а также о звуковом оборудовании. Идя по одному из задних проходов, я уловил обрывок разговора.

«Звёздный путь» прямо к вам домой

> *«Компьютер. Идентифицировать: Пикар, Жан-Люк. Кухонный свет — ВКЛЮЧИТЬ. Видеомагнитофон — ВКЛЮЧИТЬ и ЗАПИСЬ. Занавески закрыть, включить канал Ecstasy. Подготовиться к записи "Chicks with Dicks"».*
> *— Жан-Люк Пикар, звёздная дата 1992.4, 2:45 ночи*

Думаете, такое возможно только на «Звёздном пути»? Ошибаетесь. Mastervoice — «Вершина домашней автоматизации» — работает примерно как ваш личный дворецкий: сообщает точное время, активирует и управляет любым устройством в доме и даже оснащён собственной системой сигнализации. Всё это — по голосовой команде.

Mastervoice можно настроить для использования до четырёх человек и обучить на любом языке. Он различает, кто говорит, выполняет команды и — отвечает вам ЧЕЛОВЕЧЕСКИМ голосом. Мужским или женским. Можно добавлять и удалять голоса из системы распознавания, а также создавать новые ключевые слова для ответов.

Функции управления: освещение, стереосистема, телевизор, кофеварка, системы отопления и охлаждения. Плюс функция подавления бытового шума — детские игры и прочий шум в доме не мешают работе устройства.

Кроме того, это громкоговорящий телефон с памятью номеров. По голосовой команде устройство наберёт нужный номер или примет входящий звонок — и вы можете разговаривать, не прикасаясь к системе. Есть также интерфейс с ПК для хранения данных и управления.

Встроенные инфракрасный датчик и система обнаружения вторжений — ещё одна особенность этого экспоната. Система распознаёт до четырёх голосов; для каждого можно задать пароль — от «Я дома» до «Supercalafragilisticexpialidoshes». Если всё остальное не поможет — вызовет полицию сама. Полный безумный набор.

Mastervoice работает через токи несущей частоты. Эта модель относится к топовым системам голосового управления для домашнего использования и стоит от 4000 долларов, — но с учётом всего, что она умеет, оно того стоит.

Пропустив секцию игровых приставок (Nintendo/Sega/TurboGraphix и т.д.), я наткнулся на интересный карманный компьютер — Psion Series 3 и их новое программное обеспечение Interlink. Совместимый с Windows, этот наладонник оснащён не только коммуникационным ПО для связи с настольным компьютером, но и поддерживает модемы стандарта Hayes и совместимые с ним. QWERTY-клавиатура, слот для ROM-карты, 128 КБ памяти и экран на 40 столбцов — возможности Series 3 ограничены, но вполне достаточны для доступа к ряду онлайн-сервисов. На момент написания статьи доступен только пакет для Windows, однако через 5–6 месяцев должны выйти версии для DOS и UNIX.

Phrack Pro-Phile: Lex Luthor

Автор: Taran King (1986)

Добро пожаловать в Phrack Pro-Phile. Этот раздел создан для того, чтобы знакомить вас, читателей, с людьми из прошлого или особо известными и неоднозначными персонами. В этом месяце я представляю вам, пожалуй, самого знаменитого хакера андеграунда и основателя Legion of Doom.

Lex Luthor

Личное

```
        Хэндл:  Lex Luthor
   Зовите меня: Честно говоря, я больше не отождествляю себя с "Lex Luthor"
                и не ждите, что я снова буду использовать этот хэндл при
                звонках на борды — так что можете звать меня "Johnson."
 Прошлые хэндлы: Я слишком дорожил своим статусом, чтобы иметь больше одного
                хэндла. Все усилия я вложил в одну персону.
 Происхождение: Из мультсериала Superfriends/Justice League of America (ABC TV),
                где Legion of Doom (LOD) гонял их до тех пор, пока сценаристы
                не придумывали какой-нибудь нелепый способ для тех победить,
                но, конечно, LOD всегда уходил, чтобы сражаться снова.
   Дата рождения: Вы должны знать лучше, чем спрашивать об этом.
          Рост: Вы должны знать лучше, чем спрашивать об этом.
           Вес: Примерно 610 Ньютонов, плюс-минус несколько.
    Цвет глаз: С цветными контактными линзами или без?
    Цвет волос: С париком-маскировкой или без?
      Компьютер: Apple //+ покрывается пылью и скоро устаревший IBM 286.
 Email:          lex@stormking.com
```

Интервью с Lex Luthor!

Автор: Taran King

```
TK = Taran King
LL = Lex Luthor
```

TK: Итак, Lex, почему ты наконец согласился на Pro-Phile/интервью, хотя я добивался этого от тебя около 5 лет?

LL: Ну, признаю, что по-прежнему делаю это с неохотой. Вся эта тема компьютерной безопасности/незащищённости, хакинга/фрикинга, файлов/электронных публикаций и прочего остаётся весьма спорной, и я предпочёл бы сосредоточиться исключительно на законных делах. Особенно в таких областях, где мнения имеют второстепенное значение, а факты — первостепенное, как в науке и инженерии. Однако я понимаю, что Phrack существует не вечно, поэтому решил: если мне ещё есть что сказать напоследок — лучше сказать сейчас. Вот я здесь.

TK: Как ты начал заниматься хакингом/фрикингом?

LL: Это было просто. У меня был друг, который купил Apple, и я ходил к нему домой смотреть, как он играет в Ultima I — фэнтезийно-приключенческую игру. Наслюнявившись на Ultima достаточно долго, я потратил все свои сбережения и купил систему — это было свыше $1000 на тот момент. Будучи без гроша, мне было нечем заняться, кроме как изучать машину. Затем мой друг купил модем и начал звонить на борды. Я последовал его примеру. Его интересовал кряк программ, и он стал довольно известен под хэндлом "The Punk". После того как он дал мне несколько кодов для различных LD-компаний, я начал обзванивать всех подряд. Немного погодя я заметил, что существуют борды, разделы бордов и — самое главное — ИНФОРМАЦИЯ, к которой мне не разрешали получать доступ. Меня раздражало такое исключение, особенно из RACS III (Tuc в конце концов всё же допустил меня), и я взял на себя труд разобраться в том, как получить доступ к этим системам и раздобыть больше информации. Я понял, как и большинство, что обладание информацией, которой нет у других, позволяет тебя замечать и, следовательно, получать ещё больше информации. Кстати, я до сих пор играю в Ultima — купил Ultima VI два года назад, и только сейчас добираюсь до неё.

TK: Что было важнее — быть замеченным или получать информацию?

LL: Информация была, без сомнения, целью. Сейчас я понимаю, как многие хакеры и фрики осознали задним числом: я — ИНФОРМАЦИОННЫЙ НАРКОМАН. Известность была лишь средством, чтобы тебе доверяли бóльшую информацию и знания. К несчастью, тогда я не знал, что большая часть разыскиваемой мной информации была доступна ЛЕГАЛЬНО. Я был ослеплён самой информацией и не сосредотачивался на *методах её получения*. Теперь, с появлением баз данных на CD-ROM и онлайн-баз данных, информацию легко найти. Проблема в том, что поставщики услуг устанавливают цены на диски и онлайн-время, недоступные для рядовых людей, что, конечно, снова ставит меня в исходное положение.

TK: Зачем тебе нужна информация?

LL: Послушай, если есть что-то одно, что мешает людям что-то делать или преследовать свои мечты, — это ИНФОРМАЦИЯ. Не деньги, не смелость, ничто другое. Имея правильную информацию, можно получить почти всё остальное — за исключением, пожалуй, здоровья и счастья.

TK: Приведи пример.

LL: Хорошо. Если ты когда-нибудь поздно ночью смотрел телевизор и на экране появлялся какой-нибудь Дэйв Дел Дотто, Карлтон Шитс или подобный им, пытаясь продать тебе свои «курсы» по недвижимости, покупке на государственных аукционах и прочему — ты знаешь, о чём я. Эти ребята заработали миллионы, просто получив информацию, о которой большинство людей не знало, и применив её. Ими мог стать кто угодно.

TK: Какой тип информации ты ищешь?

LL: Хотя я всегда ищу новые способы получения информации в целом — какие новые базы данных доступны и как их использовать, — в настоящее время я сосредоточен на научных данных, поскольку работаю над магистерской диссертацией и мне требуется исчерпывающий обзор литературы, чтобы не дублировать уже сделанное. Философия «не изобретай велосипед заново».

TK: Ты упомянул диссертацию — какое образование у тебя есть или ты продолжаешь получать?

LL: Не хочу быть слишком конкретным, однако у меня есть степень бакалавра инженерии, и я сейчас в процессе получения двух степеней магистра — одной по квантовой физике и другой по инженерии.

TK: Звучит серьёзно. Но зачем уклоняться — должно быть, у тебя компьютерная или электротехническая специальность?

LL: Нет, и я часто слышу это от старых друзей: «Ты так хорошо разбираешься в компьютерах — почему не занимаешься этим?» Мой интерес к компьютерам теперь состоит исключительно в том, чтобы заставлять их вычислять уравнения и делать симуляции физических систем. И помогать мне получать больше информации.

TK: Вернёмся к теме X/P. Некоторые люди всегда утверждали, что ты и ребята из LOD толком ничего не знали. Это правда?

LL: Ну, я не могу много говорить о старых участниках, но их экспертиза устраивала меня и других членов (мы обычно голосовали за новых участников — я не был диктатором, знаешь ли). Что касается меня, я рано понял, что только определённым людям можно доверять определённую информацию, а некоторым типам информации нельзя доверять вообще никому. Давать полезные вещи безответственным людям неизбежно приведёт к тому, что они будут злоупотреблять этим, и вещь перестанет быть полезной. Я был очень ревнив к своей информации и часто не включал что-то в свои статьи. Не давая много данных, некоторые люди могли заключить, что я вообще ничего не знал. Просто я не выдавал это кому попало, что, вероятно, расстраивало разных людей до такой степени, что они нападали на меня и LOD.

Несколько слов о людях

Taran King: Ты вечно гонял меня за Phrack Pro-Phile. Надеюсь, ты им доволен.

Knight Lightning: Отличный парень, но как он стал таким известным, хотя даже не взламывал компьютер E911? Грустно видеть, как его подставили фанатичные «профессионалы». Жаль, что у меня не было денег, чтобы пожертвовать в его фонд защиты.

The Blue Archer: Всегда хотел познакомиться с ним. Мне так и не удалось встретиться с ним лицом к лицу, хотя я знал его 8 лет. Честно говоря, он был лучше меня в проникновении в системы.

Tuc: Всегда готов был помочь из кожи вон. Я до сих пор пользуюсь портфелем, который он купил мне в Нью-Йорке много лет назад.

Paul Muad'Dib: Тот, что из Нью-Йорка. Один из умнейших людей, которых я когда-либо встречал. Надеюсь, он занимается чем-то стоящим.

Bioc Agent 003: Разговаривал с ним немало раз и встречал на встречах TAP, но мы так и не стали друзьями.

Cheshire Catalyst: Я до сих пор должен ему $20. Он одолжил их мне в Нью-Йорке.

Control-C: Дикарь с женщинами. Надеюсь, он отдаст мне свой видеоавтомат STARGATE, когда устанет от него. Я не играю в него каждый день, как он, но всё равно могу надрать ему задницу.

Phantom Phreaker: В нём есть духовное начало, которое большинство людей никогда не замечает.

The Videosmith: Весёлый человек с талантом. Было грустно видеть, как он ушёл со сцены так рано. Встретился с ним в его родном штате два года назад — просто поздороваться.

Dr. Who: Вот человек, который любил хакинг и исследование систем. Он действительно наслаждался этим. И весьма в этом преуспел.

Telenet Bob: Встретил его в Массачусетсе на конференции Dr. Who.

Jester Sluggo: Встретил в Массачусетсе вместе с The Sprinter. Очевидно, он знал больше, чем показывал, ещё с тех давних времён.

Compu-Phreak: Мне нравилось слушать его пиратское радио, пока он его вёл. FCC так и не поймала его.

Silver Spy: Очень умный парень с будущим. Человек, который знает, когда остановиться, хотя порой немного паниковал.

Erik Bloodaxe: Часть оригинальной группы LOD. Думаю, он всегда хотел моего места. Считаю его другом, несмотря на наши разногласия.

Mark Tabas: Часть оригинальной группы LOD и сисоп Farmers of Doom (FOD) в короткое время его существования. Надеюсь, у него снова нет неприятностей.

Flash Hoser: Собрат по информационной зависимости из Великого Белого Севера (GWN).

Gary Seven: Вероятно, один из наименее известных, но при этом талантливых хакеров — за исключением того, что я упоминал его в разделе благодарностей во многих своих файлах. С тех пор он бросил.

Digital Logic: Держал хорошую борду довольно долго. Идеалист, умевший произносить прекрасные речи. Жаль, что никто не слушал.

The Ronz!: Старый друг, о котором никто никогда не слышал, если не звонил на Data Service BBS Digital Logic.

Al Capone: Нужно было родиться несколькими годами раньше, чтобы заниматься хакингом, когда это было весело. Он вошёл в это слишком поздно, и риск стал для него немного чрезмерным.

Quasi Moto: Сисоп Plovernet. Был хорошим сисопом, но не слишком сильным хакером. До сих пор общаюсь с ним в сети.

King Blotto: Знаю его давно. Рад, что он так и не поставил меня на TeleTrial!

The Mentor: Фантастический писатель. Держал отличную борду (Phoenix Project). Последний раз разговаривал с ним несколько лет назад, но он был не очень разговорчив. Думаю, он купился на старые слухи, что Lex — стукач.

The Leftist: Я подвёз его до одного из SummerCon в Сент-Луисе. С тех пор как у него начались неприятности, мы не говорили — надеюсь, он взялся за ум. Думал, что он крутой, пока не услышал, что он выдумывал обо мне что-то следователям.

The Prophet: Хакер помягче и поспокойнее. Жаль, что система его подставила.

The Urvile: Встретил его на SummerCon '89. Определённо производил впечатление человека, которому можно доверять — не подставит.

Sir Francis Drake: Встретил его на SummerCon '87. Рад, что мне представился такой случай.

Sir Knight: Ну и персонаж.

Shooting Shark: Ценю лестные слова, которые он сказал обо мне в своём Phrack Pro-Phile.

Ещё кое-что

Раз уж зашла речь о людях, есть одна вещь, которую я нигде не встречал в опубликованном виде, — это что-то вроде рубрики «Где они сейчас» для бывших хакеров/фриков. Чтобы люди знали: немало из нас весьма преуспевают в законных занятиях.

Например:

```
Silver Spy          — Заканчивает магистратуру по электротехнике.
```

```
Knight Lightning    — Работает над тем, чтобы стать юристом.
The Unknown Soldier — Менеджер высокого уровня в успешной софтверной компании.
The Mentor          — Создаёт игры в известной игровой компании.
Jester Sluggo       — Работает в «высокотехнологичной» компании.
The Disk Jockey     — Работает в компьютерном бизнесе.
Gary Seven          — Главный инженер на радиостанции.
```

Интервью с Lex продолжается

TK: В одном из ранних выпусков Phrack о тебе было сказано следующее: «Есть паранойя, а за паранойей — Lex.» Как ты на это реагируешь?

LL: Ха-ха, помню это. Ну, конечно, в этом есть доля правды. И поговорка «лучше параноик, чем потом жалеть» верна, как ты можешь видеть, — я не за решёткой... хотя, конечно, я никогда ничего незаконного не делал, хм. Стоит упомянуть, что в начале своей хакерской карьеры я встретил двух людей, оказавших на меня значительное влияние, и оба являют собой абсолютный эталон паранойи.

Первым был «Eliott Ness» — судя по голосу, ему было хорошо за тридцать или сорок. Он звонил на LOD, я познакомился с ним на местной борде. Он был чрезвычайно осведомлён, но всегда знал, когда остановиться, давая общую информацию, никогда не раскрывал НИКАКОЙ личной информации и никогда не общался долго.

Другим был «Number 6» с встреч TAP в Нью-Йорке. Я встречал его несколько раз. Шесть был ещё одним пожилым джентльменом. Он был очень спокоен, пока кто-нибудь не появлялся с камерой. Тогда он «срывался», пока угроза камеры не устранялась. Этот человек умел вытягивать из тебя информацию так, что ты даже не понимал, что происходит.

Помню, люди задавали ему вопрос, а он просто переворачивал его и говорил: «Ну, а что вы думаете (или знаете) о том-то и том-то» — и бедный фрик выкладывал всё, а Шесть делал заметки и порой поправлял то, что говорил фрик, к его немалому удивлению. Но Шесть никогда особо не раздавал информацию, хотя мне было совершенно очевидно, что он очень много знает — просто по тому, как он себя держал.

Несколько фриков пытались следить за ним после встреч TAP, но он всегда уходил от них, даже не показывая, что знает о слежке. Следует упомянуть, что паранойя может разрушить тебя (как в песне). Несколько раз я сам попадал в реальные неприятности, пытаясь уйти от подозрительных угроз, которые, вероятно, не стоили никакого беспокойства.

TK: Какие памятные H/P BBS-борды ты помнишь?

LL:

OSUNY: Застал хвост существования, когда только начинал. Был впечатлён.

Plovernet: Эта BBS была сумасшедшей. Постоянно занята, поскольку у неё были сотни активных пользователей, а Quasi Moto позволял всем постить что угодно и никогда не удалял сообщения, пока не кончалось дисковое пространство. Мы помогли запустить там тенденцию «файлов». Было легко определить, кто знал, о чём говорил, и я приглашал их на BBS LOD. Некоторых из людей на BBS LOD затем приглашали вступить в нашумевшую группу LOD.

TK: *(перебивает)* Ты когда-нибудь думал, что группа, которую ты основал, станет нарицательным именем в кругах безопасности и хак/фрик-сообщества?

LL: Хотя я знал, что ребята в группе — хорошие хакеры/фрики, я понятия не имел, к чему это приведёт. Поскольку мы не терпели деструктивного/злонамеренного поведения и таких вещей, как

мошенничество с кредитными картами, я не думал, что группе в целом грозит какое-то реальное внимание. Конечно, со временем всё изменилось.

TK: Прости за перебой. Продолжай, пожалуйста.

LL:

Metal Shop Private: Пользователи были идеалистичны и добродушны — это освежало. Мне нравилось это место больше всего, потому что там был хороший источник информации/файлов, и мы первыми видели новые выпуски Phrack.

Farmers Of Doom: Mark Tabas сделал фантастическую работу с ней. Была довольно оживлённой, но просуществовала недолго.

Phoenix Project: Снова фантастическая работа. У The Mentor были довольно нестандартные идеи — например, пускать на борду людей из сферы безопасности, что я считал хорошей идеей.

RACS III: Tuc поначалу не давал мне дня, но в конце концов я получил доступ. Потом он её закрыл.

Pirates Cove: Борда в 516 (Long Island, NY). Один из классиков. Именно там я познакомился с Emmanuel Goldstein и пригласил его на Plovernet помогать продавать подписки на 2600.

Catch-22: Абсолютно позитивно самая защищённая BBS, с которой я когда-либо сталкивался. Помимо защиты субборд паролями с требованием достаточно высокого уровня безопасности для доступа, она использовала многие концепции «базовой модели безопасности», введённой Лэмпсоном и впоследствии дополненной Грэмом и Дороти Деннинг. Конечно, Silver Spy и я понятия не имели, что такое матрица доступа и подобные вещи. Был реализован пароль принуждения: если кого-то ловили, он мог ввести этот пароль, не компрометируя систему, при этом выглядя сотрудничающим с властями, которые, как мы предполагали, попросили бы хакера позвонить. Он никогда не использовался, но было приятно его иметь.

BlottoLand: Хорошая борда какое-то время, но он пустил слишком много своих «верных подданных» — местных — и они в итоге захватили её.

TK: Ты ДЕЙСТВИТЕЛЬНО считаешь себя ЭЛИТНЫМ или как?

LL: Я правда не понимаю, откуда у кого-то взялась идея, что я считаю себя элитным. Единственные люди, которые говорили, что я так думаю о себе, — это те, с кем я никогда не встречался и не разговаривал. Вопреки некоторым убеждениям, я никогда не считал себя элитным. Я был просто парнем, который любил передавать информацию другим, поэтому писал файлы. Файлы действительно помогли мне получить доступ к большему количеству информации, сделав меня более известным. Когда я читаю газету, я — один из тех раздражающих людей, которые постоянно прерывают твой завтрак, рассказывая подробности обо всех интересных историях.

TK: Говоря о группе — что ты думаешь о том, что Erik Bloodaxe и другие создали ComSec Data Security?

LL: Когда я впервые позвонил Bloodaxe после того, как увидел их в газетах/журналах, он думал, что я буду сердит — может, что он взял мою идею или что-то в этом роде. Я сказал ему, что знаком с бизнесом консультирования по компьютерной безопасности и не хочу иметь к нему никакого отношения. Слишком сложно заставить людей платить деньги за то, от чего они не могут получить проверяемую отдачу от инвестиций. К тому же, заставить их доверять тебе свои глубочайшие секреты крайне сложно.

Я посоветовал ComSec писать статьи о безопасности, пока пальцы не отпадут. Легитимизировать себя как можно скорее. Там было слишком много предрассудков против них, и ComputerWorld вёл этот строй. Я правда думаю, что они могли бы помочь некоторым компаниям, если бы им дали шанс. Но я не думаю, что у них было достаточно знаний обо всей картине безопасности — то есть физической безопасности, инженерных систем (пожаротушение, ИБП и т.д.), административной

безопасности (политики найма/увольнения и т.д.), того, что происходит в крупных IBM-магазинах MVS, CICS, ROSCOE и т.д. Там много всего.

TK: Как ты себя чувствовал, когда Knight Lightning и Phrack по ошибке намекнули, что ты, возможно, донёс на других хакеров — может быть, даже на членов Atlanta Legion of Doom несколько лет назад?

LL: Ну, как ты теперь знаешь, Craig (KL) видел все документы и записи с его процесса и многие документы из атлантского дела — и там не было ни малейшего упоминания обо мне в связи с предоставлением информации, свидетельством, показаниями и т.д.

Хотя я не разговаривал с ребятами из Атланты со времён до их процесса, я уверен, что они знают: я не имею абсолютно никакого отношения к тому, что с ними случилось. Правдивая история с тех пор стала известна. Если есть одна вещь, которую я ненавижу, — это когда тебя обвиняют в том, чего ты не делал.

Если кто-то сделал то, в чём его обвиняют, — он должен быть достаточно мужчиной, чтобы признать это. Я говорил это уже много раз: я никогда не предоставлял никому информацию о других хакерах/фриках, которая прямо или косвенно привела бы к их визиту со стороны властей, аресту или преследованию. Это просто не мой путь. Что посеешь, то и пожнёшь, и с таким бумерангом я знал, что не хочу играть.

Мой успех в избегании неприятностей достаточно прямолинеен: прежде всего — секретность и дезинформация (в духе Stainless Steel Rat), избегание компьютеров телефонных компаний, особенно тех, клиентом которых я являлся (то есть своего местного RBOC) — потому что если ты РАЗОЗЛИШЬ их, они достанут тебя так или иначе. А также — много УДАЧИ и отсутствие намеренного создания врагов, хотя несколько хакеров злились на меня, с которыми я даже никогда не разговаривал, и у меня нет ни малейшего представления, почему я им не нравился.

TK: Есть ли у тебя советы для тех, кто хочет начать заниматься хакингом или фрикингом?

LL: Я не из тех, кто диктует людям, что им делать или не делать, но на их месте я бы не стал. Технологии предотвращения и обнаружения нарушений безопасности, а затем отслеживания их источника постоянно совершенствуются. «Яйцо кукушки» (Клиффа Столла) даёт хороший пример этого. Но это не должно быть главным аргументом.

Я думаю, им стоит объективно разобраться в том, зачем они хотят это делать. Затем честно попытаться найти другие законные способы достичь того, чего они добиваются. Как бы ты это ни оправдывал — это нечестно. Забудь о правовой стороне. Это просто создаёт проблемы другим людям. Я не знал насколько, пока системы моей школы не взломали и я не мог читать электронную почту целую неделю. Я злился и думал, что хотел бы добраться до этого придурка-хакера. Потом я долго смеялся, осознав, что думаю, и понимая всю иронию. Поэтическая справедливость, наверное. Мои данные не были тронуты, но мне отказали в обслуживании, а отказ в обслуживании может быть таким же разрушительным. Что касается самого вызова — ну, я не могу отрицать, что это было очень затягивающим, но существует много законных способов бросить себе вызов.

TK: Какие конференции/встречи за пределами телефонных звонков ты посещал?

LL: Вероятно, сначала — встречи TAP. Затем Кон в Массачусетсе, Кон в Филадельфии с Videosmith и компанией, и конечно несколько SummerCon (1987 и 1989) в Сент-Луисе. Были ещё некоторые конференции по компьютерной безопасности, которые тоже были интересны. Они помогли мне войти в положение «другой стороны».

TK: Помню, на SummerCon '89 ты случайно попал в кадр видеозаписи примерно на 2 секунды и попросил стереть это, что и было сделано. В чём дело с камерами?

LL: Это может показаться немного странным, но я не думаю, что кто-либо имеет право фотографировать другого человека без его разрешения. Особенно когда человек на плёнке не

имеет представления, где окажется фотография.

Я предсказываю, что в течение максимум 5–10 лет штаты начнут использовать видеокамеры для оцифровки фотографии при получении новых водительских прав. Оцифрованное изображение будет храниться вместе с остальной личной информацией и, вероятно, будет доступно таким людям, как частные сыщики, и другим, получающим к информации незаконный доступ. С ISDN, мультимедиа и прочим можно будет очень легко «подставить» людей, изменяя изображения с помощью компьютеров так, чтобы они выглядели делающими практически что угодно. Когда такие вещи начнут происходить, я буду выглядеть не сумасшедшим, а умным — по крайней мере, в глазах друзей, считающих моё избегание камер ненормальным.

Самые памятные события

TK: Какие у тебя самые памятные переживания (смешные или не очень вещи, случившиеся во время фрикинга/хакинга или в другое время)?

LL: Dr. Who в Массачусетсе организовал конференцию, на которую мы с Tuc и The Videosmith ехали в 4 часа утра на жуке Tuc, аквапланируя всю дорогу из-за дождя и смертельно уставшие. Все мы были в дурацком настроении и много смеялись.

Ещё — время, когда я был в Нью-Йорке с Paul Muad'Dib, и у нас не было денег на еду. Он был первым из знакомых мне людей, кто обладал реальными знаниями о коммутационных системах телефонных компаний. Он перепрограммировал коммутатор на Манхэттене, поставив переадресацию вызовов на таксофон. После этого все деньги, опущенные в телефон, оставались в нём, но не падали в монетный ящик. Те, кто опускал деньги, по сути не должны были этого делать, поскольку телефон был преобразован в POTS (Plain Old Telephone Service). Увы, люди — существа привычки. Так что через пару часов (так как телефон был оживлённым) он попросил парня вернуть телефон в исходное состояние. Когда это было сделано, все деньги, задержанные в телефоне, вернулись. Это было как сорвать джекпот в Лас-Вегасе. Затем мы отправились в McDonald's.

История о том, как я бегал голым по стоянке Motel 6, которую Control-C пытался заставить людей принять за правду, разумеется, сильно преувеличена. Его подруга познакомила меня со своей приятельницей. Дэн и его девушка были в другом номере. Он позвонил мне прийти, но я был в нижнем белье. Мы немного выпили, поэтому я пробежал 8 или около того футов до его номера (мы были на 2-м этаже с глухим балконом, так что с земли никто всё равно не видел), сказал привет и побежал обратно в свой номер продолжать.

Пожалуй, самое любимое воспоминание относительно недавнее. Дж. Дж. Блумбекер, директор Национального центра данных по компьютерным преступлениям, выступал в моей школе. Я сидел в самом дальнем ряду, как обычно (терпеть не могу, когда кто-то сидит позади меня — где бы то ни было), в аудитории примерно на 40 человек и слушал его речь, которая в основном была направлена на продвижение его книги «Spectacular Computer Crimes». Я говорил с ним, но так и не открыл, кто я на самом деле. Он говорил о деле Craig'a (Knight Lightning), а затем высказался о том, кто бы ни назвал LOD, Legion of Doom, — следовало назвать их чем-то вроде «Legion of Ineffectual Pansies». Причина в том, что какой прокурор в здравом уме пойдёт к судье и будет доказывать опасность группы бесполезных нытиков.

Я сидел, стараясь не краснеть, и думал, что из всех сотен людей, которым он это говорил, он, вероятно, никогда не ожидал сказать это человеку, который действительно дал группе это название.

Я дважды встречал Донна Б. Паркера, которого считаю отцом компьютерной безопасности. В первый раз просто пожал ему руку. Второй раз был относительно недавно — мы говорили около 20 минут. Я так и не сказал ему, кто я на самом деле, — хотя он всё равно бы не знал. Но я достаточно его похвалил, так что даже если бы он узнал, не смог бы сильно на меня злиться.

TK: Какие из твоих памятных достижений (рассылки/файлы и т.д.) ты бы выделил?

LL: Настоящие достижения (не файлы) останутся анонимными, но мои любимые файлы — это серия IBM VM/CMS, потому что они были хорошо написаны, а также серия об атаках, преодолении и обходе физических средств безопасности. Прежде чем написать файл, я прочёсывал борды и другие традиционные источники в поисках нужной информации. Если приходил ни с чем — исследовал тему и писал сам.

Хотя файлы COSMOS помогли мне начать, они были совершенной шуткой. Они давали достаточно информации, чтобы быть опасными, и не помогали моим отношениям с RBOC. Файлы VAX/VMS становились лучше по мере развития, но за исключением части III они не давали ничего, чего не было бы в руководствах. Я люблю писать, но обычно мне нужно много правок, чтобы довести до ума. Что касается рассылок — LOD/H Technical Journal — это ещё одна вещь, в которой я принимал участие.

TK: Что стоит за LOD/H Technical Journal?

LL: LOD/H Technical Journal едва не остался несостоявшимся. Как ты знаешь, LOD собрал группу файлов для публикации в PHRACK в качестве «выпуска полностью от LOD», но некоторые участники считали, что нам стоит выпускать собственный материал. Идея мне понравилась, и я сказал «хорошо». Стоит упомянуть, что ты помог нам с первым выпуском — проверял правописание, редактировал и критиковал. Но мы смогли выпустить только 4 номера, так как было трудно получать качественный непиратский и не перефразированный до неузнаваемости материал.

После третьего выпуска я понял, что, вероятно, не оказываю никому никакой услуги, раскрывая дыры в безопасности и слабые места систем. Некоторые люди могут не поверить, слыша это от МЕНЯ, но я не согласен с теми хакерами, которые думают, что оказывают людям услугу, раскрывая уязвимости их систем. Никому не нужно, чтобы кто-то ночью проверял, заперта ли их дверь. И хотя старая аналогия с дверью не совсем то же самое, что псевдофизический компьютерный логин, — достаточно близко. Извини, что немного отошёл от темы.

TK: Ничего. Почему ты ушёл из H/P-сообщества?

LL: Около года назад я написал письмо в журнал 2600, где немного касаюсь этого. Между тем письмом и тем, что я сказал здесь, должно быть достаточно очевидно. Вкратце: я понял, что занимался этим в основном ради получения информации. Это стало слишком опасным, и я решил направить свою энергию на окончание учёбы, а не на то, как обходить системы защиты. Мыслительные процессы, задействованные в хакинге, и те, что используются при решении задач инженерного проектирования, поразительно похожи, и я думаю, что мой опыт хакинга делает меня значительно лучшим проектировщиком и решателем проблем. Это не реклама — в поисках работы я не нахожусь...

Любимые вещи Lex'a

```
Женщины: Без болезней.
 Машины: Такие быстрые, что страшно жать педаль в пол.
   Еда:  Всё, что не содержит пестицидов, гербицидов, тяжёлых металлов,
         радиоактивных элементов, токсичных химикатов, вредных
```

```
          микроорганизмов, искусственных красителей или консервантов.
          Думаю, это исключает рыбу, сельхозпродукты, мясо,
          обработанные продукты, питьевую воду и так далее.
          Иными словами — есть больше нечего. Если серьёзно, я люблю
          большие салаты, и если бы был богатым — у меня был бы шикарный
          винный погреб.
Музыка: Heavy Metal, немного панка и классика.
Авторы: Richard P. Feynman, Isaac Asimov, Stephen Hawking, Jane Roberts,
        Budd Hopkins, Jacques Valee, Bruce Sterling, K. Eric Drexler,
        Matthew Lesko.
Книги:  «Яйцо кукушки», всё о физике и неконъюнктурные метафизические
        книги. Единственное, что я коллекционирую в наши дни, — это книги.
        Их у меня сотни.
Игры:  Atari's ASTEROIDS DELUXE — вероятно, самая сложная видеоигра
       из когда-либо созданных (хотя ей уже больше десяти лет), и в ней
       я один из лучших в мире. Вот здесь признаю — я ЭЛИТНЫЙ.
       Почти никто на планете не может меня победить.
       Defender и Stargate тоже великолепны. Больше таких игр не делают.
       И конечно — серия Ultima.
Актёры: Dana Carvey, Bill Moyers, Patrick Stewart (ST:TNG), Jonathan Frakes
        (ST:TNG), Andy Griffith (Matlock) и слишком много кинозвёзд,
        чтобы всех перечислять.
```

Интервью завершается

TK: Есть ли кто-то конкретный, кому ты хочешь что-то сказать?

LL: Всем тем, кто придерживается менталитета «однажды вор — всегда вор», и тем немногим упорным блюстителям закона, которые были бы рады добраться до меня и других бывших хакеров: не беспокойтесь — люди в основе своей хороши и могут быть «реабилитированы» без тюрьмы.

Другое, чего я никогда не понимал в хак/фрик-сообществе, — это некоторая одержимость слежкой за людьми. Я мог бы понять это немного лучше, когда причиной была проверка других на то, что они не являются федералами.

Я никогда не составлял списков тех, с кем общался, — только хэндл, имя и телефон. Я никогда не пробивал их через CNA на фамилии и не пытался выяснить, где они работают.

Но некоторые ребята просто должны были знать всё обо всех. Им что, больше нечем заняться? Я был осторожен — да, но не настолько, чтобы вторгаться в личную жизнь каждого, особенно когда человек говорил, что хочет, чтобы его оставили в покое. Я не говорю, что НИКОГДА не нарушал чужую частную жизнь, но сейчас не делаю этого и в прошлом почти никогда не делал.

Я оставил адрес электронной почты в начале этого Pro-Phile, чтобы люди могли связаться со мной. Я не против общения с людьми, но просто не считаю справедливым преследовать и угрожать людям, которые не хотят, чтобы их беспокоили. Я открыт для полезных и конструктивных разговоров по электронной почте, но действительно не думаю, что необходимо составлять досье на частных лиц. Я этого никогда не делал и никогда не пойму, зачем люди это делают.

К тому же найти людей в наши дни — не великое достижение. Способов получить информацию много, и многие из них законны — так что много ли умения требуется, чтобы узнать чью-то информацию? Почти никакого. Это может сделать кто угодно... о ком угодно.

TK: Что ты думаешь о будущем хак/фрик-мира или телекоммуникаций в целом?

LL: Что касается хак/фрик-аспекта: каждый раз, когда я думаю, что хакинг мёртв и нужно быть психом, чтобы взламывать компьютеры или бесплатно звонить незаконно, я читаю об очередном бедолаге или группе бедолаг, которые это сделали. Неужели они не понимают, что есть лучшие и более простые способы добиться того, что они хотят? Неужели они не понимают, что технология

для того, чтобы ПОЙМАТЬ тебя, такова, что ты проиграл бой ещё до того, как начал?

Да, появятся новые технологии, которые помогут обеим сторонам, но здесь действует закон убывающей отдачи. Что касается того, что хакеры должны делать, — если и делать что-то, то следить за нашим правом на частную жизнь. Если бы не хакеры, TRW до сих пор бы обирал людей (хуже, чем сейчас) и никогда бы не извинился за то, что не исправлял недействительную кредитную информацию.

TK: И, конечно, вопрос, без которого не обходится ни один Phrack Pro-Phile...

Из общего числа фриков, которых ты встречал, — считаешь ли ты большинство из них, если вообще кого-либо, компьютерными задротами?

LL: Абсолютно НЕТ. Я больше не сужу о людях по внешности (хотя раньше делал это). Как The Mentor так красноречиво выразил в своём Манифесте хакера (Phrack 7 и снова в Phrack 14), из которого это — лишь жалкий пересказ: важнее соотносить людей с тем, что они знают и каковы их идеи, чем с их внешностью или цветом кожи и т.д. И подавляющее большинство имеет совсем не задротские идеи.

TK: Спасибо за твоё время, Lex.

LL: Спасибо, что дал мне столько болтать.

Сетевые заметки: Как получить информацию об интернет-компьютерах

Автор: The Racketeer (Hellfire Club)

Составлено из интернет-источников

Рубрика Network Miscellany создана Taran King

Вообще говоря, информация — это всё. Большая часть хакинга любого компьютера в сети строится на умении собирать данные о машине и её уязвимостях. Этот файл посвящён использованию доступных ресурсов сети Интернет для получения важной информации о любом интересующем сайте.

В последнее время в Phrack было опубликовано немало материалов об Интернете, большей частью скопированных прямо из руководств и, на мой взгляд, лишённых хакерской искры. Поэтому я сразу возьму быка за рога и расскажу вам о сборе информации по существу!

Интернет печально известен отсутствием руководства пользователя. Большинство людей узнают, что такое Интернет, от друзей. Когда-то единственным настоящим ориентиром в Интернете был FTP-архив SIMTEL-20. Сегодня Интернет — вероятно, крупнейшая бесплатная сеть в мире. По сути, это настоящий рай для хакера!

К сожалению, прежде чем воспользоваться «публичными» узлами сети, нужно знать о их существовании. И как вы собираетесь взламывать организацию, если не знаете ни одной из её машин? Это всё равно что пытаться пожаловаться в Packard-Bell на неисправное оборудование, когда эти ребята не указывают ни названия, ни адреса, ни телефона. Придётся найти другой способ добыть нужную информацию.

Не существует какого-то одного верного метода разузнать всё о сайте. На самом деле придётся сочетать несколько нестандартных способов сбора информации, чтобы получить что-то похожее на «полную картину». Однако, используя комбинацию техник, описанных в этом файле, вы сможете ориентироваться в любой сети Интернета и узнавать о машинах, входящих в её состав.

ARPANet Network Information Center (NIC)

Первая остановка в нашем путешествии — ARPANet Network Information Center (опытные пользователи сети обычно называют его просто «NIC»). Назначение NIC — вести учёт всех сетевых подключений, полей, доменов и хостов, сведения о которых люди хотят сделать общедоступными.

Чтобы подключиться к NIC, с вашей машины, имеющей доступ в Интернет, нужно ввести примерно такую команду:

```
                .---------------------- команда
               \/
[lycaeum][1]> telnet nic.ddn.mil
```

Вскоре это направит вас в Сетевой информационный центр и предоставит доступ. Привычной системы входа/выхода, как на других Unix-машинах, здесь нет — вы сразу попадаете в информационную систему. Приветственное сообщение будет выглядеть примерно так:

```
*  -- DDN Network Information Center --
*
*  For TAC news, type:                    TACNEWS <return>
*  For user and host information, type:   WHOIS <return>
```

```
*  For NIC information, type:             NIC <return>
*
*  For user assistance call (800) 235-3155 or (415) 859-3695
*  Report system problems to ACTION@NIC.DDN.MIL or call (415) 859-5921

 SRI-NIC, TOPS-20 Monitor 7(21245)-4
@ <prompt>
```

Отлично, мы внутри. По сути, NIC — это огромная телефонная книга, и нам нужно как следует в ней покопаться. Давайте продемонстрируем несколько простых команд на примере одного из гигантов государственного подряда — корпорации UNISYS. Начнём с ввода WHOIS.

```
@WHOIS
SRI-NIC WHOIS 3.5(1090)-1 on Tue, 22 Aug 91 15:49:35 PDT, load 9.64
  Enter a handle, name, mailbox, or other field, optionally preceded
  by a keyword, like "host sri-nic".  Type "?" for short, 2-page
  details, "HELP" for full documentation, or hit RETURN to exit.
---> Do ^E to show search progress, ^G to abort a search or output <---
Whois:
```

Хорошо, теперь мы в базе данных. Поскольку наша цель — Unisys, запросим информацию о «Unisys».

```
Whois: unisys

Cartee, Melissa (MC142)         unisys@email.ncsc.navy.mil     (904) 234-0451
Ebersberger, Eugen (EE35)       UNISYS@HICKAM-EMH.AF.MIL       (808) 836-2810
Lichtscheidl, Mark J. (MJL28)   UNISYS@BUCKNER-EMH1.ARMY.MIL   (DSN) 634-4390
Naval Warfare Assessment Center (UNISYS) UNISYS.NWAC.SEA06.NAVY.MIL
                                                                 137.67.0.11
Navratil, Rich (RN74)           UNISYS@COMISO-PIV.AF.MIL       (ETS) 628-2250

There are 28 more matches.  Show them?  y      -->  конечно

Peterson, Randy A. (RP168)      UNISYS@AVIANO-SBLC.AF.MIL      (ETS) 632-7721
Przybylski, Joseph F. (JP280)   UNISYS@AVIANO-SBLC.AF.MIL      (ETS) 632-7721
UNISYS Corporation (BIGBURD)    BIGBURD.PRC.UNISYS.COM          128.126.10.34
UNISYS Corporation (GVLV2)      GVL.UNISYS.COM                128.126.220.102
UNISYS Corporation (MONTGOMERY-PIV-1) MONTGOMERY-PIV-1.AF.MIL      26.5.0.204
Unisys Corporation (NET-MRC-NET)MRC-NET                          192.31.44.0
Unisys Corporation (NET-SDC-PRC-CR) UNISYS-ISF-11                192.26.24.0
Unisys Corporation (NET-SDC-PRC-LBS) UNISYS-ISF-9                192.26.22.0
UNISYS Corporation (NET-SDC-PRC-NET) UNISYS-ISF-7               192.12.195.0
Unisys Corporation (NET-SDC-PRC-SA) UNISYS-ISF-10                192.26.23.0
Unisys Corporation (NET-SDC-PRC-SW) UNISYS-ISF-8                 192.26.21.0
Unisys Corporation (NET-UNISYS-CULV) UNISYS-CULV                 192.67.92.0
Unisys Corporation (NET-UNISYS-PRC) UNISYS-PRC                   128.126.0.0
Unisys Corporation (NET-UNISYS-RES1) UNISYS-RES1                 192.39.11.0
Unisys Corporation (NET-UNISYS-RES2) UNISYS-RES2                 192.39.12.0
Unisys Corporation (NET-UNISYS2)UNISYS-B2                        129.221.0.0
Unisys Corporation (STARS)      STARS.RESTON.UNISYS.COM         128.126.160.3
Unisys Corporation (UNISYS-DOM)                                    UNISYS.COM
Unisys Linc Development Centre (NET-LINC) LINC                   143.96.0.0
UNISYS (ATC-SP)                 ATC.SP.UNISYS.COM             129.218.100.161
Unisys (FORMAL)                 FORMAL.CULV.UNISYS.COM           192.67.92.30
UNISYS (KAUAI-MCL)              KAUAI.MCL.UNISYS.COM            128.126.180.2
UNISYS (MCLEAN-UNISYS)          MCLEAN-UNISYS.ARMY.MIL             26.13.0.17
UNISYS (NET-UNISYS-RES3)        UNISYS-RES3                      192.67.128.0
Unisys (NET-UNISYS-SP)          UNISYS-SP                        129.218.0.0
UNISYS (SALTLCY-UNISYS)         SALTLCY-UNISYS.ARMY.MIL          26.12.0.120
UNISYS (SYS-3)                  SYS3.SLC.UNISYS.COM            129.221.15.85
Wood, Roy (RW356)               UNISYS@LAKENHEATH-SBLC.AF.MIL
                                              0044-0638-522609 (DSN) 226-2609
```

Как видите, информация об этих компьютерах довольно подробна. Первый «столбец» — совпавшие данные, второй — сетевое имя или заголовок, затем следует номер телефона или IP-адрес. Если у телефонного номера есть код города, значит это обычная телефонная линия; если же указано (DSN) — это «Data Security Network», она же Autovon (военная телефонная система).

Как видно из приведённого списка, у военных машин имеется несколько учётных записей UNISYS — в том числе военная машина, НАЗВАННАЯ в честь Unisys (mclean-unisys.army.mil). Это объяснимо, поскольку Unisys занимается преимущественно военным компьютерным оборудованием. Казалось бы, для секретной военной структуры посторонний не должен получить много информации.

Вот что происходит, когда запрашиваешь конкретного человека:

```
Whois: cartee
Cartee, Melissa (MC142)            unisys@email.ncsc.navy.mil
   7500 McElvey Road
   Panama City, FL 32408
   (904) 234-0451
   MILNET TAC user

   Record last updated on 18-Apr-91.
```

Хм... Весьма интересно. Этот пользователь, очевидно, имеет доступ к военным компьютерам, поскольку располагает TAC-картой, и в целом действует под псевдонимом «Unisys». Не является ли эта персона связующим звеном между Unisys и Министерством обороны США? Вполне возможно. Скорее всего, она — контактное лицо по техническому обслуживанию, поскольку TAC-карта позволяет ей подключаться к нескольким (закрытым) военным сетям.

Теперь я запросил конкретную информацию о kauai.mcl.unisys.com — судя по всему, это узловой сервер сетей Unisys. Конечно, сведения о нём не засекречены (а если засекречены, дядюшка Сэм, скорее всего, уже устроил Unisys нагоняй). Обратите внимание на обилие полезной информации:

```
Whois: kauai.mcl.unisys.com
UNISYS (KAUAI-MCL)
   Building 8201, 10th Floor Computer Room
   8201 Greensboro Drive
   McLean, VA 22102

   Hostname: KAUAI.MCL.UNISYS.COM
   Nicknames: MCL.UNISYS.COM
   Address: 128.126.180.2
   System: SUN-3/180 running SUNOS

   Coordinator:
      Meidinger, James W.  (JWM3)  jim@BURDVAX.PRC.UNISYS.COM
      (215) 648-2573

   domain server

   Record last updated on 05-Aug-91.

   No registered users.
```

Ага! Координатор этой машины ею не пользуется! Зарегистрированных пользователей нет! Иными словами, если захотите её взломать, вы не потревожите начальство (а это хорошо). С каких пор Unisys покупает компьютеры у других компаний? Неужели не могут взять несколько штук прямо с конвейера? Компьютер находится в Маклине, Вирджиния! А там расположено ЦРУ! Неужели Unisys разрабатывает компьютеры для международного шпионажа? Очевидно, с этой машины можно выудить массу информации.

Как? Ответ уже есть в полученных данных. Машина является ДОМЕННЫМ СЕРВЕРОМ. Это означает, что на ней хранится сетевая информация, идентифицирующая все компьютерные системы в её сети, и нам осталось лишь найти способ эту информацию извлечь! Но сначала проверим нашу догадку о том, что большие шишки далеко, — взглянем на главного координатора, «мистера Мейдингера».

```
Whois: jim@burdvax.prc.unisys.com
Meidinger, James W. (JWM3)             jim@BURDVAX.PRC.UNISYS.COM
   Unisys Corporation
```

```
Computer Resources
Room g311
P.O. Box 517
Paoli, PA 19301-0517
(215) 648-2573

Record Last Updated on 04-Jul-90.
```

Точно так. Мистер Мейдингер далеко — если быть точным, в Пенсильвании. До клавиатуры явно не дотянется. К тому же, работая в отделе «Computer Resources», он, скорее всего, просто бухгалтер. Бухгалтеры в вычислительной технике — как бобры среди деревьев (если только им самим не нравятся компьютеры, что в деловом мире вовсе не очевидно).

Про остальные возможности NIC я умолчу — в этом журнале о нём и так уже всё исписано. Единственная подсказка: читайте новостные заметки CERT и DDN, там встречается немало полезных и познавательных сведений. К тому же возиться с наёмниками ЦРУ куда интереснее.

Доменные серверы и nslookup

Небольшой урок критического мышления: Интернет — не совсем «общедоступная» сеть в том смысле, что нельзя просто подключить свой компьютер к какой-нибудь машине в Интернете и ожидать, что всё само заработает. Нужно настроить машину под компьютеры того сетевого домена, к которому вы подключаетесь, и получить на это разрешение. Но как только вы настроены и ваш маршрутизатор и/или сервер узнал о вашем существовании — означает ли это, что эта информация есть у всех остальных? Да, хотя до NIC она не дойдёт — её придётся получать другим способом.

Все пакеты данных в Интернете маршрутизируются между корректными компьютерными хостами. Поэтому вся эта информация хранится на шлюзе сети. Однако маршрутная информация представлена лишь в числовом формате, например 128.126.160.3. По крайней мере, это ещё понятно — Ethernet-адреса и вовсе гораздо сложнее и в двоичном виде.

Тем не менее, как знают пользователи Интернета, описать компьютер можно не одним способом. Подключиться к машине можно командой «telnet 128.126.160.3» или «telnet aviary.stars.reston.unisys.com» — это одна и та же машина. Имена выбирает владелец сети; они описываются с помощью «доменных серверов».

Как мы помним, NIC указал kauai.mcl.unisys.com как доменный сервер. Это означает, что имена компьютерных систем данной сети хранятся именно на этом хосте. Конечно, это не единственная его функция. Доменный сервер предоставляет подключающейся машине имя компьютера и его IP-номер, позволяя подключаться к нему по «доменному имени». В конечном счёте всё сводится к IP-номерам.

Большинство сетевых программ поддерживает совместимость с доменными серверами: если хотите подключиться к nic.ddn.mil и вводите команду «telnet nic.ddn.mil», то подключитесь именно к nic.ddn.mil. К сожалению, не все компьютеры это поддерживают (некоторые принимают только IP-номера), но большинство обычных пользователей имеют доступ к подобным ресурсам.

Из глубины веков существует программа, позволяющая машинам, которые не умеют напрямую преобразовывать доменные имена в IP-адреса, всё же узнавать имя машины. Программа называется «nslookup» и обычно находится в операционной системе Unix (по крайней мере, я нигде больше её не встречал — возможно, она работает только под Unix).

«nslookup» расшифровывается как Name Server Lookup (существуют споры о том, является ли доменный сервер на самом деле именным сервером или наоборот; оба термина достаточно точно описывают суть, что и порождает путаницу). Так или иначе, давайте научимся пользоваться

nslookup.

```
[lycaeum][2]> nslookup
Default Name Server:  lycaeum.hfc.com
Address:  66.6.66.6
```

Вернёмся к полученным ранее данным NIC и продолжим изучать добрый старый Unisys, который сдаёт нам информацию на каждом шагу. Мы определили, что kauai.mcl.unisys.com является доменным сервером, поэтому переключимся на него — ведь интересующие нас компьютеры находятся не у нас.

```
> server kauai.mcl.unisys.com
Default Server:  kauai.mcl.unisys.com
Address:  128.126.180.2
```

Теперь мы подключены к серверу. Оговорюсь: это не постоянное соединение. Связь устанавливается лишь на короткий момент выполнения команд. Пароль или учётная запись для получения информации с именного сервера не требуются.

Начнём с запроса обо всём, что известно этому серверу об Unisys. «Всё» — отличная отправная точка, ошибиться здесь невозможно. Если ничего не найдётся — значит, ничего и нет. Базовая команда для получения списка машин — «ls», как команда каталога в Unix.

```
> ls unisys.com
[kauai.mcl.unisys.com]
Host of domain name            Internet address
 unisys.com                     server = burdvax.prc.unisys.com         3600
 burdvax.prc.unisys.com         128.126.10.33                   3600
 unisys.com                     server = kronos.nisd.cam.unisys.com     3600
 kronos.nisd.cam.unisys.com     128.170.2.8                     3600
 unisys.com                     server = kauai.mcl.unisys.com           3600
 kauai.mcl.unisys.com           128.126.180.2                   43200
 unisys.com                     server = io.isf.unisys.com              3600
 io.isf.unisys.com              128.126.195.20                  3600
 reston.unisys.com              server = aviary.stars.reston.unisys.com 3600
 aviary.star.reston.unisys.com  128.126.160.3                   3600
 aviary.star.reston.unisys.com  128.126.162.1                   3600
 reston.unisys.com              server = kauai.mcl.unisys.com           3600
 kauai.mcl.unisys.com           128.126.180.2                   43200
 rosslyn.unisys.com             server = aviary.stars.reston.unisys.com 3600
 aviary.stars.reston.unisys.com 128.126.160.3                   3600
 aviary.stars.reston.unisys.com 128.126.162.1                   3600
 rosslyn.unisys.com             server = kauai.mcl.unisys.com           3600
 kauai.mcl.unisys.com           128.126.180.2                   43200
 rmtc.unisys.com                server = rmtcf1.rmtc.unisys.com         3600
 rmtcf1.rmtc.unisys.com         192.60.8.3                      3600
 rmtc.unisys.com                server = gvlv2.gvl.unisys.com           3600
 gvlv2.gvl.unisys.com           128.126.220.102                 3600
 sp.unisys.com                  server = dsslan.sp.unisys.com           3600
 dsslan.sp.unisys.com           129.218.32.11                   3600
 sp.unisys.com                  server = sys3.slc.unisys.com            3600
 sys3.slc.unisys.com            129.221.15.85                   3600
 cam.unisys.com                 server = kronos.nisd.cam.unisys.com     3600
 kronos.nisd.cam.unisys.com     128.170.2.8                     3600
 cam.unisys.com                 server = burdvax.prc.unisys.com         3600
 burdvax.prc.unisys.com         128.126.10.33                   3600
 prc.unisys.com                 server = burdvax.prc.unisys.com         3600
 burdvax.prc.unisys.com         128.126.10.33                   3600
 prc.unisys.com                 server = kronos.prc.unisys.com          3600
 kronos.prc.unisys.com          128.170.2.8                     3600
 prc.unisys.com                 server = walt.prc.unisys.com            3600
 walt.prc.unisys.com            128.126.2.10                    3600
 walt.prc.unisys.com            128.126.10.44                   3600
 culv.unisys.com                server = formal.culv.unisys.com         3600
 formal.culv.unisys.com         192.67.92.30                    3600
 culv.unisys.com                server = kronos.nisd.cam.unisys.com     3600
 kronos.nisd.cam.unisys.com     128.170.2.8                     3600
 slc.unisys.com                 server = sys3.slc.unisys.com            3600
 sys3.slc.unisys.com            129.221.15.85                   3600
```

```
 slc.unisys.com                server = dsslan.sp.unisys.com          3600
 dsslan.sp.unisys.com          129.218.32.11                  3600
 slc.unisys.com                server = nemesis.slc.unisys.com        3600
 nemesis.slc.unisys.com        128.221.8.2                    3600
 bb.unisys.com                 server = sunnc.wwt.bb.unisys.com       3600
 sunnc.wwt.bbs.unisys.com      192.39.41.2                    3600
 bb.unisys.com                 server = burdvax.prc.unisys.com        3600
 burdvax.prc.unisys.com        128.126.10.33                  3600
 isf.unisys.com                server = orion.ISF.unisys.com          3600
 orion.ISF.unisys.com          128.126.195.7                  3600
 isf.unisys.com                128.126.195.1                  3600
 isf.unisys.com                server = burdvax.prc.unisys.com        3600
 burdvax.prc.unisys.com        128.126.10.33                  3600
 isf.unisys.com                server = io.isf.unisys.com             3600
 io.isf.unisys.com             128.126.195.20                 3600
 gvl.unisys.com                128.126.220.102                172800
 gvl.unisys.com                server = gvlv2.gvl.unisys.com          3600
 gvlv2.gvl.unisys.com          128.126.220.102                3600
 gvl.unisys.com                server = burdvax.prc.unisys.com        3600
 burdvax.prc.unisys.com        128.126.10.33                  3600
 mcl.unisys.com                128.126.180.2                  43200
 mcl.unisys.com                server = kauai.mcl.unisys.com          43200
 kauai.mcl.unisys.com          128.126.180.2                  43200
 mcl.unisys.com                server = burdvax.prc.unisys.com        43200
 burdvax.prc.unisys.com        128.126.10.33                  3600
 mcl.unisys.com                server = kronos.nisd.cam.unisys.com    43200
 kronos.nisd.cam.unisys.com    (dlen = 1152?)                 4096
ListHosts: error receiving zone transfer:
  result: NOERROR, answers = 256, authority = 0, additional = 3.
```

Обидно, ошибка. Забавно, что ошибка не признаётся ошибкой, однако сервер споткнулся на адресе kronos и выбросил нас вон. Видимо, доменный сервер сломан. Ну да ладно — это уже их проблема, потому что в полученной информации есть всё необходимое для следующего шага!

Быстрый анализ показывает, что большинство серверов были связаны как минимум с двумя другими. Весьма внушительно: отказоустойчивая TCP/IP-сеть. Раз она отказоустойчива, можно использовать другую машину, чтобы заглянуть в домен «mcl.unisys.com». Поскольку «mcl» обозначает McLean — туда нам и нужно.

Помните, NIC сообщил, что у kauai.mcl.unisys.com есть псевдоним? Он также известен как «mcl.unisys.com». В приведённом выше списке, ближе к концу, видно, что mcl.unisys.com также обслуживается доменными серверами burdvax.prc.unisys.com и kronos.nisd.cam.unisys.com. Подключимся к одному из них!

Когда сервер начинает чудить, как kauai, я предпочитаю использовать IP-номера там, где они доступны. Подключусь к burdvax.prc.unisys.com по его IP-адресу 128.126.10.33.

```
> server 128.126.10.33
Default server: [128.126.10.33]
Address:  128.126.10.33
```

Теперь, когда мы подключены, снова запросим сетевую информацию, но на этот раз попробуем кое-что другое и, возможно, более полезное. Используем ключ -h, который описывает тип процессора (CPU) и операционную систему (OS) каждой машины — это даст нам более чёткое представление о том, с чем мы имеем дело.

```
> ls -h mcl.unisys.com
Host or domain name           CPU          OS
 maui.mcl.Unisys.COM           SUN-2/120    UNIX        43200
 cisco.mcl.Unisys.COM          CISCO GATEWAY CISCO             43200
 kauai.mcl.Unisys.COM          SUN-3/180    UNIX        43200
 voyager.mcl.Unisys.COM        SUN-4/330    UNIX        43200
 dial.mcl.Unisys.COM           SUN-3/260    UNIX        43200
 astro.mcl.Unisys.COM          SUN-3/60     UNIX        43200
 hotrod.mcl.Unisys.COM         Unisys 386   SCO/UNIX            43200
 oahu.mcl.Unisys.COM           VAX-11/785   UNIX        43200
 lanai.mcl.Unisys.COM          SUN-3/160    UNIX        43200
```

```
mclean_is.mcl.Unisys.COM      386          NOVELL              43200
```

ВАУ! Сколько Sunов! Похоже, Unisys совершенно не доверяет собственным компьютерам! Интересно, что сказал бы президент Буш об этой демонстрации корпоративной веры в свой продукт! Единственный компьютер Unisys во всём этом зоопарке — дешёвый клон 386, который, скорее всего, стоит на чьём-то рабочем столе.

И снова здесь масса интересного. Пробежимся по списку:

Maui — Sun 2, весьма старый RISC-компьютер. Их уже почти не осталось, однако для хранения данных они ещё могут пригодиться. Хотя, с другой стороны, он, вероятно, быстрее среднего PC!

Oahu — Vax-11, судя по всему работающий под Ultrix. Возможно, здесь Unisys собрал всех своих программистов, поскольку машина не используется для серьёзной сетевой работы (по крайней мере, судя по имеющимся данным).

Mclean_is — файловый сервер для PC-сети. Сколько компьютеров подключено к этой сети, отсюда не видно, однако вполне возможно, что она служит для публичного обмена информацией, где секретари и администраторы подтверждают торговые операции и расписания.

Hotrod — тоже 386, причём производства самой Unisys! Но странно: на нём установлен SCO Unix, а значит это, без сомнения, личная машина кого-то, кто занимается Unix-программированием. Если бы Unisys была частью правительства, я бы решил, что этот компьютер — результат халтурного тендера по минимальной цене.

Voyager — интересная машина, судя по всему самая современная в сети. Как Sun-4 (вероятно, IPX) она является высокопроизводительной графической рабочей станцией. Возможно, здесь хранятся и используются многочисленные CAD-приложения. Другой вариант: Sun 4 стоили бешеных денег, когда эту сеть Sunов только покупали, и эта машина была приобретена как файловый сервер для остальных Sun 3 и Sun 2. Получив доступ к одной из остальных машин, вы, вероятно, получите доступ ко всем.

Cisco — стандартный маршрутизатор/шлюз Cisco, связывающий эту сеть с Интернетом.

Kauai — сломанный доменный сервер, и ладно. Возможно, он работает в одной сети с Astro и Lanai.

Dial — Sun-3. Может, название что-то значит? Это вполне может быть телекоммуникационный узел дозвона в сеть. Возможно, на том же компьютере есть модем для исходящих звонков. Не исключено даже наличие гостевой учётной записи для входящих пользователей, чтобы они могли легко подключаться к другим компьютерам в сети (хотя это вряд ли).

Astro и Lanai — тоже Sun 3. Их назначение не вполне очевидно. Скорее всего, все они были куплены примерно в одно время (чем объясняется обилие Sun-3 в этой сети) и вполне могут быть просто подключены к Sun 4 в рамках единой файловой сети. Также возможно, что они старше и являются фундаментом коммуникационной платформы Unisys на данном объекте.

Ограничения флага -h

У использования ключа -h есть один изъян: иногда люди понимают, что это возможно, и удаляют информацию об отдельных машинах в сети или изначально её не вносят. Поэтому всегда лучше выполнять «ls \» и проверять всё, на случай если машина была удалена. Подключение через «telnet» — безотказный способ узнать, что именно за компьютер находится по тому или иному адресу.

```
> ls mcl.unisys.com
[[128.126.10.33]]
Host or domain name             Internet address
```

```
mcl.Unisys.COM                  server = kauai.mcl.unisys.com         3600
kauai.mcl.unisys.com            128.126.180.2                 3600
mcl.Unisys.COM                  server = burdvax.prc.unisys.com       3600
burdvax.prc.unisys.com          128.126.10.33                 3600
mcl.Unisys.COM                  server = kronos.nisd.cam.unisys.com   3600
kronos.nisd.cam.unisys.com      128.170.2.8                   3600
mcl.Unisys.COM                  128.126.180.2                 43200
maui.mcl.Unisys.COM             128.126.180.3                 43200
cisco.mcl.Unisys.COM            128.126.180.10                43200
kauai.mcl.Unisys.COM            128.126.180.2                 3600
voyager.mcl.Unisys.COM          128.126.180.37                43200
dial.mcl.Unisys.COM             128.126.180.36                43200
LOCALHOST.mcl.Unisys.COM        127.0.0.1                     43200
astro.mcl.Unisys.COM            128.126.180.7                 43200
hotrod.mcl.Unisys.COM           128.126.180.125               43200
oahu.mcl.Unisys.COM             128.126.180.1                 43200
lanai.mcl.Unisys.COM            128.126.180.6                 43200
mclean_is.mcl.Unisys.COM        128.126.180.9                 43200
```

Пройдясь по списку, замечаем, что других важных для этого домена компьютеров, которых мы ещё не знаем, здесь нет. LOCALHOST — просто ещё один способ сказать «подключись к тому, где находишься», так что ничего интересного. Hotrod, судя по IP-адресу x.x.x.125, явно обособлен от остальных машин — похоже на наспех сделанную проводку, скорее всего для отдельного офиса, как я и предполагал.

Следующий шаг

Что дальше? Взламывайте! Именно здесь пригождаются все те системные эксплойты, которыми обмениваются в сети, и все те Бюллетени CERT. Если вы хорошо разбираетесь во взломе какого-то типа машин (например, Sun), nslookup поможет идентифицировать эти машины и упростит работу.

Искать компьютеры-аннексы, библиотечные серверы, гостевые машины и прочее тоже легко с nslookup — имена и типы машин у вас перед глазами. Предварительный отбор интересных «узкоспециализированных» машин с помощью nslookup может дать отличные результаты. Люди называют это «нетраннингом» — и название, пожалуй, ничуть не хуже любого другого.

Разумеется, другая большая проблема при работе с доменными серверами — их обнаружение. Самый полный список доменных серверов можно найти в Перечне сетей Министерства обороны (обычно называемом hosts.txt), который доступен практически повсюду в Интернете через анонимный FTP. Вот как получить этот файл:

```
[lycaeum][3]> ftp wuarchive.wustl.edu

220 wuarchive.wustl.edu FTP server (Version 6.24 Fri May 8 07:26:32 CDT 1992)
ready.
Remote host connected.
Username (wuarchive.wustl.edu:rack): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password (wuarchive.wustl.edu:anonymous):
230-  This is an experimental FTP server.  If your FTP client crashes or
230-  hangs shortly after login please try using a dash (-) as the first
230-  character of your password.  This will turn off the informational
230-  messages that may be confusing your FTP client.
230-
230-  This system may be used 24 hours a day, 7 days a week.  The local
230-  time is Wed Jun  3 20:43:23 1992.
230-
230-Please read the file README
230-  it was last modified on Mon Mar  2 08:29:25 1992 - 93 days ago
230-Please read the file README.NFS
230-  it was last modified on Thu Feb 20 13:15:32 1992 - 104 days ago
230 Guest login ok, access restrictions apply.
```

```
ftp> get /network_info/hosts.txt
200 PORT command successful.
150 Opening ASCII mode data connection for /network_info/hosts.txt (1088429 bytes).
226 Transfer complete.
Transferred 1109255 bytes in 182.95 seconds (6063.29 bytes/sec, 5.92 KB/s).

ftp> quit
221 Goodbye.
```

Теперь преобразуем его в файл, с которым удобно работать: извлечём из огромного списка только машины, являющиеся доменными серверами:

```
[lycaeum][4]> grep -i domain hosts.txt > domains
```

Готово. Докажем, что это способ найти доменный сервер, не подключаясь ни к чему. Воспользуемся grep для поиска по файлу серверов в домене mcl.unisys.com:

```
[lycaeum][5]> grep -i mcl.unisys.com domains
HOST : 128.126.180.2 : KAUAI.MCL.UNISYS.COM,MCL.UNISYS.COM : SUN-3/180 :
SUNOS : TCP/TELNET,TCP/FTP,TCP/SMTP,UDP/DOMAIN :
[lycaeum][6]>
```

Вот ещё один способ. Всё, что мы получали раньше, здесь тоже есть: IP-номер, имя, псевдоним, тип компьютера, операционная система и краткий список поддерживаемых сетевых протоколов, включая атрибут доменного сервера. Однако остальные машины из сети mcl.unisys.com здесь не отображаются. Список MO — не полный реестр сетевых машин, а лишь те из них, которые жизненно важны для функционирования Интернета (за последний год этот список вырос примерно с 350 КБ до 1,1 МБ — и это отражает только «новые» сети, без учёта добавления новых машин в уже существующие; Интернет явно «в тренде»; по некоторым оценкам, рост составляет 25% в месяц!).

Очевидно, это особенно эффективно при работе с университетскими сайтами: у них слишком много машин, чтобы уследить за безопасностью каждой. По сути, список MO содержит примерно ту же информацию, что и NIC, но примерно в миллион раз более дискретен. Не знаю, полностью ли ведётся журнал NIC, но там точно есть штатный руководитель службы безопасности (*смешок*).

Ну что ж, на этом, пожалуй, закончим. Надеюсь, кое-что из сказанного окажется вам полезным.

Бухта Пиратов

Автор: Rambone

Добро пожаловать обратно в Бухту Пиратов. Приношу свои извинения за то, что не подготовил эту колонку для Phrack 39. Однако в этом выпуске мы рассмотрим несколько недавних облав на пиратские борды и организацию, которую следует винить во всём этом... Ассоциацию издателей программного обеспечения (Software Publishers Association). Помимо этого — новости и информация о Vision-X, обзоры игр, журнал BAD и многое другое. Приятного чтения.

ФБР совершает налёт на компьютерного пирата; SPA подаёт гражданский иск — 11 июня 1992 года

БОСТОН — Федеральное бюро расследований провело [10 июня] обыск в «Davy Jones Locker» — компьютерной доске объявлений, расположенной в Миллбери, штат Массачусетс, которая предположительно незаконно распространяла защищённые авторским правом программы.

Доска объявлений Davy Jones была сложной компьютерной системой с платными подписчиками в 36 штатах и 11 зарубежных странах.

Компьютерная доска объявлений позволяет пользователям персональных компьютеров получать доступ к главному компьютеру через телефон с модемом для обмена информацией, включая сообщения, файлы и программы. Системный оператор (или сисоп) несёт ответственность за материалы, размещённые на борде.

За плату в размере $49 на три месяца или $99 на год подписчики Davy Jones Locker получали доступ к специальному разделу, который содержал копии более 200 защищённых авторским правом программ, включая популярные деловые и развлекательные пакеты. Подписчики могли «скачивать» или получать эти программы для использования на своих компьютерах, не платя ничего правообладателю.

Деловые программы предлагались от ряда хорошо известных компаний, в том числе: AutoDesk, Borland International, Broderbund, Central Point System, Clarion Software, Fifth Generation, Fox Software, IBM, Intuit, Lotus Development, Micrografx, Microsoft, Software Publishing Corp., Symantec, Ventura Software, WordPerfect и X-Tree Co. Развлекательные программы включали Flight Simulator от Microsoft и Leisure Suit Larry от Sierra.

В ходе обыска в Davy Jones Locker были изъяты компьютеры, телекоммуникационное оборудование, а также финансовые и прочие документы.

«SPA аплодирует действиям ФБР сегодня», — заявила Илин Розентал, директор по судебным делам Ассоциации издателей программного обеспечения (SPA). «Это один из первых известных нам случаев, когда ФБР закрыло пиратскую доску объявлений за распространение программ, защищённых авторским правом. Это явно свидетельствует о тенденции: правительство осознаёт серьёзность нарушения авторских прав на программное обеспечение. Примечательно также, что на этой неделе Сенат принял S.893 — законопроект, криминализирующий незаконное распространение защищённого авторским правом ПО как уголовное преступление».

В течение последних четырёх месяцев Ассоциация издателей программного обеспечения проводила расследование в отношении доски объявлений Davy Jones Locker и скачивала с неё

деловые и развлекательные программы. Полученные с Davy Jones Locker программы затем сравнивались с оригинальными материалами, защищёнными авторским правом. Во всех случаях они оказались идентичными.

Подписчики Davy Jones Locker не только скачивали защищённое авторским правом программное обеспечение, но и поощрялись к размещению на доске дополнительных защищённых программ.

Системный оператор ограничивал пребывание подписчиков на борде до четырёх часов в сутки. Он также ограничивал количество программного обеспечения, которое подписчик мог скачать на свой компьютер за день. Те, кто «заливал», то есть передавал на борд новые защищённые авторским правом программы для дальнейшего незаконного распространения, получали кредиты на дополнительное онлайн-время или дополнительное программное обеспечение.

«Представьте видеомагазин, который берёт с вас членский взнос, а затем позволяет незаконно копировать защищённые авторским правом фильмы на чистые видеокассеты», — объясняет Илин Розентал, директор SPA по судебным делам. «Но при этом ограничивает число фильмов, которые вы можете скопировать, если только вы не принесёте новые — копии новых фильмов, которых ещё нет на полках. Вот что происходило в Davy Jones Locker».

Davy Jones Locker была международной системой с платными подписчиками в Соединённых Штатах и 11 зарубежных странах, включая Австралию, Канаду, Хорватию, Францию, Германию, Ирак, Израиль, Нидерланды, Испанию, Швецию и Великобританию.

Вне зависимости от того, скопирована ли программа с диска, купленного в ближайшем компьютерном магазине, или скачана с борда за тысячи миль, пиратское ПО увеличивает стоимость компьютинга. По данным SPA, программные пираты по всему миру похищают от 10 до 12 миллиардов долларов в виде защищённого авторским правом программного обеспечения ежегодно.

«Многие люди, возможно, не осознают, что цены на программное обеспечение выше отчасти для того, чтобы компенсировать потери от пиратства», — говорит Кен Уош, исполнительный директор SPA. «Пиратские доски объявлений не только распространяют деловое программное обеспечение, но и наносят вред издателям компьютерных игр, незаконно распространяя так много их программ. Кроме того, они подрывают репутацию сотен легитимных досок объявлений, которые выполняют важную функцию для пользователей компьютеров».

Ассоциация издателей программного обеспечения является основной торговой ассоциацией отрасли программного обеспечения для персональных компьютеров. Её 900 членов представляют ведущих издателей на рынках делового, потребительского и образовательного программного обеспечения. SPA имеет офисы в Вашингтоне, О.К., и в Париже Ля Дефанс, Франция.

КОНТАКТ: Software Publishers Association, Вашингтон, О.К.
Терри Чайлдс или Илин Розентал, 202/452-1600

PC-борда подверглась налёту ФБР — 14 июня 1992 года

Автор: Josh Hyatt (Boston Globe)(Chicago Tribune, раздел 7, стр. 3)

БОСТОН — В одном из первых зафиксированных случаев подобного рода шесть агентов ФБР на прошлой неделе провели обыск в компьютерной доске объявлений, располагавшейся в жилом доме в Миллбери, штат Массачусетс. Власти заявили, что оператор борды незаконно распространял программное обеспечение, защищённое авторским правом.

Исполняя уголовный ордер на обыск, агенты изъяли несколько компьютеров, шесть модемов и программу под названием PC Board, использовавшуюся для управления бордой. Также были изъяты документы со списком пользователей сервиса.

Арестов не производилось, сообщила Ассоциация издателей программного обеспечения — торговая группа, которая передала дело в ФБР. По оценкам ассоциации, по состоянию на март борда распространила защищённое авторским правом программное обеспечение на сумму $675 000; по её же данным, программные пираты таким образом похищают до $12 миллиардов ежегодно.

ФБР отказывается комментировать дело, за исключением подтверждения факта обыска и продолжения расследования. Предполагаемый оператор борды Ричард Кенадек оказался недоступен для комментариев.

Приблизительно в то же время, что и обыск, ассоциация издателей подала против Кенадека гражданский иск, обвинив его в нарушении законов об авторском праве. Илин Розентал, директор группы по судебным делам, сообщила, что «мужчина изобличил себя сам» через различные компьютерные сообщения.

«Есть более чем достаточно доказательств того, что он прекрасно знал обо всём, что происходило на его борде», — сказала она.

Доски объявлений позволяют пользователям персональных компьютеров получать доступ к главному компьютеру через модемы. Как правило, участники обмениваются информацией обо всём — от компьютерных программ до тропических рыбок. Они также могут, например, получать обновления компьютерных программ.

Ассоциация заявила, что её собственное четырёхмесячное расследование показало: данная борда, известная как Davy Jones Locker, содержала копии более 200 защищённых авторским правом программ.

Розентал сообщила, что пользователей также поощряли загружать защищённое авторским правом программное обеспечение для скачивания другими.

По словам Розентал, подписчики платили взнос: $49 на три месяца или $99 на год. Она сообщила, что у Davy Jones Locker было почти 400 платных подписчиков в 36 штатах и 11 зарубежных странах.

Наступление на компьютерных фальшивомонетчиков — июль 1992 года

Автор: B.A. Nilsson (PC-Computing Magazine)(стр. 188)

Популярные ритуалы сближения обычно не являются уголовно наказуемыми. Восхититесь новым автомобилем друга — и вы, скорее всего, обменяетесь парой историй и банкой STP. Вас могут пригласить прокатиться. Вы можете обмениваться рецептами или одолжить другу свой экземпляр последнего бестселлера.

Обмен компьютерными программами — ещё одна распространённая практика среди друзей. Здорово помочь кому-то, кого пугает перспектива освоения новой машины, и иногда это включает в себя подарок из любимого программного обеспечения. «На, начни с WordPerfect». И позже, неизбежно: «Norton Utilities вернёт тебе этот файл».

Скопировать набор дисков так просто и так приватно, что едва ли задумываешься о том, что это также незаконно. О юридической стороне вопроса легко забыть. Уведомление об авторских правах — сложная штука, которую нередко печатают на запечатанной упаковке программного обеспечения, что срывается при извлечении флоппи-дисков. Вы можете даже не быть тем, кто

вскрывал оригинальную упаковку (в таком случае вы — ещё один из тех, кто «нагрел» программу).

Но осознаёте вы это или нет — если вы не вскрывали упаковку лично или не получили её со всеми дисками, документацией и лицензионной информацией в целости, вы нарушаете закон. Хорошая новость: если вы частное лицо с пиратским ПО на домашнем компьютере, вас, вероятно, не поймают. Но если вы начальник с обозлённым сотрудником, Ассоциация издателей программного обеспечения (SPA) может получить наводку. Когда SPA приходит к вашей компании — это с маршалами США и кучей официальных бумаг. И у ассоциации раздражающе успешная история победы в делах о нарушении авторских прав.

Взгляды на пиратство

«Компьютеры дают нам своего рода техническую изощрённость, которой раньше не существовало», — говорит Кен Уош, словоохотливый руководитель SPA. «В старые времена, если вы хотели сделать собственную копию чего-то вроде карандаша, вам понадобился бы сложный производственный центр. Но сам факт того, что вы можете запустить компьютерную программу, означает, что вы можете сделать её безупречную копию. Это единственная отрасль в мире, которая наделяет каждого покупателя возможностями производственного дочернего предприятия».

Правила снова и снова прописаны в руководствах по программному обеспечению: вам разрешено делать одну или две копии программы для резервных целей. Остальные правила немного различаются от компании к компании. Некоторые лицензионные соглашения требуют, чтобы программный пакет использовался только на одной машине; другие, наиболее известные — Borland, позволяют использовать программу на скольких угодно компьютерах, при условии что никакие две копии не запускаются одновременно — подобно тому, как книгу одновременно может читать лишь один человек.

«Если бы все разработчики программного обеспечения придерживались того же подхода, что и Borland International, люди не воровали бы так много», — говорит убеждённый пират Эд Тич.

(Примечание: имена и местонахождение всех опрошенных пиратов изменены.)

«Borland даёт вам книжную лицензию. Конечно, они доведут вас до безумия обновлениями. Они отдают программное обеспечение оптом, а потом зарабатывают на всех последующих релизах».

Тич является системным администратором жилищно-медицинской компании на юго-востоке страны. «Я верю в пиратство», — говорит он. «Мне нравится что-нибудь взять поиграть. Если понравится — куплю».

Он отвергает демо-версии и ограниченные варианты программ как неадекватные для его предпочтений в тестировании; точно так же он считает типичное 30-дневное соглашение о возврате слишком ограничительным. «Это нереальный период для оценки», — говорит Тич. «Я только что получил копию FormTool Pro, а это мощная программа с очень крутой кривой обучения. Я не могу посвятить себя ей и узнать всё необходимое за 30 дней».

Тич провёл шесть лет, рекомендуя и настраивая программы для своей компании. Он не вписывается в образ нарушителя закона и убеждён, что то, что он делает, морально оправдано. «В конечном счёте я покупаю программное обеспечение. Моя компания купила лицензии на использование WordPerfect 5.1, начав с пиратской копии программы. Всё на корпоративных машинах — легальное».

Копирование не всегда было таким простым. Старожилы помнят схемы защиты от копирования, пронизывавшие компьютерную отрасль и требовавшие ключевых дисков или специальных процедур инициализации. Но пользователи единогласно потребовали положить этому конец, и когда Lotus — последний значимый противник — сдался, та эпоха закончилась. Сегодня защиту можно найти лишь в играх и нишевых программах.

Во сколько обошлось программным компаниям исчезновение защиты от копирования? Точно подсчитать невозможно. В августе 1991 года неутомимая Ассоциация издателей программного обеспечения опубликовала данные о корпоративных потерях от использования, свидетельствующие как об огромных финансовых потерях, так и о возможном снижении пиратства. В 1987 году на каждый офисный компьютер продавалось 1,31 программного обеспечения для DOS. Ожидаемое соотношение — три пакета на компьютер, то есть более половины используемых программ, вероятно, были пиратскими. В 1990 году количество легальных пакетов выросло до 1,78. Но цены тоже выросли, так что финансовые потери практически не изменились: ответственность 1987 года составляла $2,3 миллиарда, а к 1990 году число выросло до $2,4 миллиарда.

С другой стороны, цифры пиратства в частном пользовании не поддаются подсчёту. Если бы все пользователи компьютеров, никогда не занимавшиеся пиратством, собрались вместе, им не понадобился бы большой зал. Уош признаёт, что реально поймать и привлечь к ответственности индивидуального пирата затруднительно. «Никто на самом деле не сидит за пиратство», — говорит он, упоминая в качестве исключения розничного торговца, которого поймали за ведением чего-то вроде магазина пиратского программного обеспечения.

Программная полиция

Хотя SPA изучает домашнее нарушение в текущем исследовании, Уош считает, что наибольшие финансовые потери обусловлены корпоративным пиратством. Корпоративных пиратов легче поймать, потому что озлобленный сотрудник нередко готов сдать начальника. «Мы получаем около 20 звонков в день», — говорит Уош, который открыл специальный номер (800-388-7478) для сообщений о пиратстве. «Девяносто процентов звонков, которые мы отрабатываем, поступают от недовольных сотрудников».

Это визит, который большинство из нас видели только в кино, и он, как правило, неожиданный. Администратор одной из целевых компаний была настолько потрясена прибытием отряда SPA, что спросила, не «Скрытая камера» ли это.

Основанная в 1984 году как образовательная и промоционная группа, SPA пять лет назад эволюционировала в программную полицию по мере того, как всё больше поставщиков программного обеспечения вступало в её ряды. Сейчас их почти 800. SPA начала всерьёз привлекать информаторов около двух лет назад, после того как наводка привела к успешному аресту крупной корпорации на Среднем Западе.

«Дела идут слишком хорошо», — говорит Уош. «Мы ведём гораздо больше судебных исков и аудитов, чем когда-либо прежде, и цифры продолжают расти».

Если вашу корпорацию поймала SPA, молитесь, чтобы это произошло по почте. «Тогда мы пишем директору письмо, объясняя, что хотим провести аудит», — говорит Уош. «Если мы найдём нелегальное программное обеспечение, компания платит дважды: один раз за пиратскую копию, один раз за новую.

«Для компании это куда лучше. Штраф значительно меньше, и они не сталкиваются с негативной оглаской, которая возникает из-за судебного иска. Тем не менее 60 процентов из них обещают не уничтожать программное обеспечение до составления отчёта, а потом всё равно делают это».

Именно так произошло при недавнем визите SPA к компании среднего размера из оборонного сектора в Вашингтоне, О.К. «Они согласились на аудит, а затем попытались стереть пиратские программы со всех жёстких дисков», — говорит Уош. «Но мы знали. Почему они думали, что мы позвонили им в первую очередь? Кто-то изнутри говорил. Не могу поверить, что они смотрели мне в глаза и врали — мы держали их за горло!»

Всё более зловещий призрак SPA, вышибающей двери, заставляет многие компании переходить на легальное ПО, хотя некоторые продолжают придумывать отговорки. «Я не хочу нарушать закон, но и не хочу разоряться», — говорит Хауэлл Дэвис, директор бухгалтерской фирмы в столице Новой

Англии. «Мы не можем работать без компьютеров, но я не могу платить высокую цену за регистрацию каждой копии каждой программы, которую мы используем. Мне пришлось занять немало денег, чтобы запустить этот бизнес, и я воспринимаю это как ещё одну форму займа. Это ещё один заём, который я верну, когда смогу себе это позволить».

Некоторые корпоративные пираты действуют с ощущением полной вседозволенности.

«Никто нас не поймает», — говорит Чарльз Вэйн, управляющий директор некоммерческого театра на северо-западе. «И никто даже не должен пытаться. Мы на грани банкротства. Компании должны дарить нам программные пакеты в знак поддержки искусства». Он признаёт, что почти всё программное обеспечение его театра пиратское. «У нас есть хорошие программы, включая бухгалтерский пакет, разработанный для Ernst & Young, который мы стащили, и копию SuperCalc с кучей дополнительных модулей. И WordPerfect, конечно», — говорит Вэйн.

Откуда берутся пакеты? «Наши члены совета директоров добывают их для нас», — говорит Вэйн. «Конечно, это означает, что мы не можем быть привередливы. Нам приходится ждать, пока конкретная программа попадёт к нам. А больше всего они любят давать нам игры. У нас миллион игр».

Игры и пиратство — естественные партнёры. Игры сами поощряют пиратство. В отличие от деловых программ, они порождают интенсивные, недолгосрочные отношения. Или, как выражается оператор пиратского BBS Джон Рэкхем: «Игры надоедают. Вот почему на пиратских бордах их так много».

Онлайн-пиратство

Рэкхем управляет BBS прямо из «Человека из У.Н.К.Л.Е.». Она выглядит как любая другая борда среднего размера в стране — стандартная коллекция шароваре и базы сообщений. Получите особый доступ — для этого достаточно $50 и рекомендации друга — и вы пройдёте через секретную дверь в коллекцию объёмом 600 МБ из новейших приложений, включая 10 zip-файлов с полным dBASE IV, 11 — с AutoCAD и 6 — с MS-DOS 5.0.

«Большинство людей, которые пользуются моей бордой, — коллекционеры», — говорит он. «Им нужна последняя копия всего». Рэкхема не пугает угроза поимки. «Я не думаю, что это случится со мной. Я не делаю ничего по-настоящему ужасного. То есть, я не рублю тела или что-то вроде того. Я не получаю с этого денег. Плата — только для поддержания оборудования. Я считаю себя библиотекарем».

Novell смотрит на подобное отношение неодобрительно, о чём свидетельствует обыск в августе 1991 года на двух калифорнийских BBS-системах, обвиняемых в распространении файлов Novell NetWare. Такие системы — ещё одна цель, по которой SPA хотела бы ударить, и Уош ищет сотрудничества с ФБР.

Это делает сеть Humble Guys созревшей для удара. Изучите высокочёткий GIF-файл этих буканьеров — и вы увидите собрание обычно выглядящих людей, которые занимаются торговлей пиратским игровым программным обеспечением. Основатель — хакер, называвший себя Candy Man, — уже давно покинул страну; теперь у руля стоит The Slave Lord, студент одного из южных колледжей.

«Вся суть сети — получить игры раньше, чем они появятся в магазинах», — говорит Билл Кидд, компьютерный консультант на Манхэттене. «Это что-то вроде доказательства мужественности — насколько быстро ты можешь их достать». Кидд заявляет, что лично мало причастен к пиратству, но знает, где зарыты тела.

«Сначала есть поставщики, которые могут получить программу от производителя задолго до её выхода», — говорит Кидд. «Нередко поставщик работает на производителя. Игра поступает к главному человеку, который передаёт её крэкерам. Именно они снимают защиту от копирования.

Оттуда она идёт к курьерам, у каждого из которых есть список пиратских BBS. Затем программа распространяется по всей стране за считанные минуты».

Скорость — это одержимость. Эти пираты вооружены модемами на 9600 бит в секунду и менталитетом «надо прямо сейчас». «За неделю до того, как MS-DOS 5.0 появился в магазинах», — говорит Кидд, — «большинство пиратских бордов уже удалили его, потому что предлагали бета-версии за шесть месяцев до этого».

Что касается доходов, пиратские доски объявлений, возможно, являются скорее неудобством, чем угрозой. «Эти люди никогда по-настоящему не купят это программное обеспечение», — говорит Джон Ричардс, менеджер по продукту в Lotus. «Формально это плохо, но не то чтобы они покупают одну копию 1-2-3, чтобы установить её на рабочую станцию офиса для десяти пользователей».

Пираты дома

В то время как офисная среда позволяет проводить регулярные тщательные аудиты, домашний пользователь безнаказанно пиратит программное обеспечение. Загляните под крышку нескольких жёстких дисков — и вы непременно найдёте что-нибудь незаконное.

«Это может произойти вполне невинно», — говорит Род Тёрнер из Symantec. Как генеральный менеджер Peter Norton Group, Тёрнер имеет честь курировать одно из наиболее часто пиратируемых программ: Norton Utilities. «Кто-то устанавливает копию программного обеспечения на чужую машину, чтобы попробовать, и забывает убрать. Другой пользователь предполагает, что она там законно», — говорит Тёрнер.

«Нередко кто-то получает программное обеспечение от друга, который взял его на работе», — говорит Тони Гир, менеджер по сервису в Computer Directions — розничном магазине в Олбани, Нью-Йорк. Гир ежемесячно просматривает сотни пользовательских жёстких дисков. «Кто-то покупает у нас машину, а потом звонит и говорит, что у него теперь есть куча программного обеспечения — не могли бы мы объяснить, как его запускать», — говорит Гир. «Что мне делать? Клиент хочет, чтобы я провёл с ним часы по телефону и обучил его, иначе он злится. Когда я говорю, что ему нужно ещё и купить программу, он раздражается».

Гир также получает огромное количество запросов на пиратское программное обеспечение. «Многие пользователи думают, что мы можем загрузить их жёсткие диски программами, даже зная, что должны за них платить, и просто хотят уклониться от платы».

Несколько запросов поступает от действительно наивных людей, говорит Гир. «Мне звонят за поддержкой программного обеспечения, и я спрашиваю: что говорит руководство? — Руководства у меня нет, — отвечает человек. — Мне это дал друг. — И тогда мне приходится объяснять, что программное обеспечение не бесплатно».

Высокие цены на программное обеспечение — распространённая жалоба пользователей. Тем не менее бывший исполнительный вице-президент WordPerfect У.И. «Пит» Петерсон считает цену $495 за лучшую программу обработки текстов WordPerfect оправданной. «WordPerfect продаётся около 150 000 копий в месяц по этой цене, так что немало пользователей тоже считают её оправданной», — говорит Петерсон. «Компьютер стоит от нескольких сотен до нескольких тысяч долларов. Без программного обеспечения компьютер бесполезен. WordPerfect прилагает огромные усилия, чтобы написать и поддерживать программное обеспечение».

Последнее включает в себя дорогостоящую политику бесплатной телефонной поддержки, которую ведут операторы, предпочитающие не спрашивать регистрационный номер. Это дорогостоящий способ демонстрации доверия, но он окупился отличными связями с общественностью.

«Мы стараемся проявлять сочувствие к людям», — говорит Джефф Кларк, директор по связям с общественностью в XyQuest — компании, выпускающей XyWrite, программу обработки текстов, популярную среди журналистов. «Мы продаём сменные руководства зарегистрированным

пользователям как услугу, но не реже раза в неделю поступает звонок от кого-то, кто явно пытается получить руководства к пиратской копии».

Задача тогда — просветить звонящего, который, возможно, даже не знает, что нарушил закон. «Всё, что мы просим у зарегистрированного пользователя, — запускать программу на одной машине одновременно», — объясняет Кларк. «Если вы пользуетесь ею на работе — да, можете дома. Но не покупайте одну копию для использования в офисе из восьми человек».

«Многие, кажется, думают, что копировать диски нормально, потому что это легко», — говорит Тёрнер, который также является председателем сопутствующей организации SPA — Business Software Alliance, борющейся с международным пиратством. «Потом они звонят на нашу техническую линию, и мы оказываемся в деликатном положении, сообщая им, что они незаконно используют продукт».

Microsoft ещё более снисходительна. «Нам нравится знать, откуда взялась пиратская копия», — говорит Билл Поуп, заместитель генерального юрисконсульта компании. «Не всегда возможно узнать по телефону, кто пиратит что-то, потому что мы не требуем возврата регистрационных карточек. Но если мы обнаруживаем пиратскую копию, мы поможем пользователю получить её законно и даже можем предоставить бесплатную копию программы, если сможем выяснить, откуда она взялась».

Широко разрекламированная программа амнистии была запущена компанией XTree в июле 1982 года. За $20 любой обладатель пиратской копии программы XTree мог купить лицензию на базовую версию программы, получив тем самым доступ к пути обновлений. В течение 90-дневного периода отклик был enthusiastic, но предложение больше не будет повторяться. «Нельзя раз за разом предлагать амнистию», — говорит Майкл Калин, занимающийся маркетингом продуктов XTree. «Теряешь уважение дилеров и пользователей, заплативших полную цену».

Тёрнер более прямолинеен. «Амнистия поощряет пиратство. Я не думаю, что это было успешно».

Пока SPA продолжает попадать в заголовки газет с налётами в стиле «Неприкасаемых» на корпоративные офисы, Уош также признаёт, что ключом к борьбе с пиратством является образование. 12-минутный видеоролик «It's Just Not Worth the Risk», созданный SPA, доносит послание через образ добродушного корпоративного менеджера, которого просвещают о пиратстве в компании.

«Этот ролик имел огромный успех», — говорит Уош. «American Express купил 300 копий, а Kimberly-Clark только что заказал 100. Мы распространили уже около 10 000 копий».

Набор для самоаудита, также доступный от SPA, включает программу, которая определяет, какое программное обеспечение используется на вашем ПК, а также образцы корпоративных служебных записок и форм соглашений с сотрудниками для повышения осведомлённости о пиратстве.

Прозрение

Страх быть пойманным удерживает многих людей от нарушений, но некоторые пираты будут ждать, пока их не заставят пройти по доске, прежде чем сдаться.

Джон Рэкхем говорит, что его пользователи невиновны. «Они не могут позволить себе программное обеспечение, и они не должны платить», — говорит он. «Они скачивают. Распаковывают архив и говорят: — О, неплохо! — А потом больше никогда этим не пользуются».

Чарльз Вэйн считает, что компании-разработчики программного обеспечения должны дать послабление некоммерческим организациям вроде его театра. «Если они дадут нам пакеты, мы дадим им рекламу. Напечатаем в программке, разместим в фойе. К нам приходит публика высокого класса. Нам просто не хватает денег. Я купил одну программу — ReportWriter — потому что она была дешёвой и хорошей».

Для случайных пользователей пиратство может быть просто фазой. «Я владею 90 процентами программ, которые использую», — говорит системный администратор Эд Тич. «Это большой откат от примерно четырёх лет назад, когда 90 процентов из них были пиратскими».

И всегда остаётся проблема добросовестных друзей. Генри Эвери, журналист флоридской газеты, получил пиратские программы от друзей, когда пять лет назад купил свой первый компьютер.

«У меня были все эти программы, и я понятия не имел, как ими пользоваться», — говорит Эвери. «К счастью, в книжном магазине нашлись руководства, которые оказались даже лучше официальных, и я стал своего рода продвинутым пользователем. Потом я сам стал тем, кому звонил друг друга, чтобы попросить помощи с машиной. И вот я уже сам раздаю пиратские копии.

«Но больше я этого не делаю. Мне надоели звонки в любое время дня и ночи с просьбами объяснить, как пользоваться этими чёртовыми программами».

Отговорки не принимаются

«Когда я сижу с ними за одним столом и они выглядят по-настоящему виноватыми, когда вижу белки их глаз, трудно нажать на курок», — говорит Кен Уош, глава Ассоциации издателей программного обеспечения. «Тем не менее», — говорит он, — «я нажимаю».

Уош не нежный человек в обращении с пиратами программного обеспечения. У него нет терпения к типичным отговоркам тех, кто копирует и использует нелицензионное программное обеспечение, и он предлагает следующие ответы на распространённые жалобы, которые слышит от нарушителей:

• **Цена слишком высокая.**

«Слушай, у меня нет Mercedes Benz. Почему? Цена слишком высокая. Если ты не можешь себе позволить — не пользуйся».

• **Лучше тестировать настоящую вещь, чем урезанную или демо-версию.**

«Демо-версии обычно очень хорошие. Они ограничивают количество записей, или не сохраняют на диск, или что-то ещё. Этого достаточно».

• **Я заплачу потом.**

«Сомневаюсь».

• **Меня не поймают.**

Уош смеётся. Когда он смеётся, невольно хочется надеяться, что он смеётся вместе с тобой, а не над тобой. «Рано или поздно...»

Как Microsoft перехитрила пиратов

Имитация — лесть, только когда это не стоит вам денег. Многие программные пакеты копируются ловкими пиратами, дублирующими диски, руководства и даже упаковку. Microsoft страдала от фальшивомонетчиков достаточно часто, чтобы последние выпуски программного обеспечения — в том числе обновления Windows 3.1 и MS-DOS 5.0 — были специально разработаны защищёнными от пиратства.

«Каждый компонент был тщательно разработан или отобран вручную именно по этой причине», — говорит Кристи Бэнкхед, работающая с генеральным советником Microsoft по вопросам пиратства. «Для пользователя это должно выглядеть просто как привлекательная коробка, но это позволяет нам немедленно определить, законная ли она».

Эта стратегия окупилась в марте, когда агенты ФБР провели обыск в четвёрке компаний Силиконовой долины, зарабатывавших до $600 000 в месяц на распространении поддельных копий MS-DOS и Windows.

Ключевые элементы официальных дизайнов коробок, защищённых от пиратства, — красочное оформление и использование голограмм. На коробке обновления MS-DOS 5.0 серебряный кружок сбоку предлагает переливающееся изображение логотипа. Вторая голограмма — небольшой прямоугольник на боку руководства к программе — просвечивает через дорогое фигурное отверстие с другой стороны коробки. Переплетённые буквы D-O-S напечатаны четырёхцветным способом, дающим сложные смеси, которые невозможно воспроизвести. Даже способ складывания коробки и склейки клапанов уникален — это не распространённый стиль, и фальшивомонетчики должны либо потратить время и деньги на его копирование, либо рисковать быстрым разоблачением.

Ещё когда пакет обновлений DOS готовился к выходу на рынок в прошлом году, полицейские детективы обнаружили базировавшуюся в Лос-Анджелесе пиратскую группировку, уже работавшую над полноразмерными подделками. «Мы застали их в процессе завершения работы над оформлением DOS 5.0», — сказала Бэнкхед, — «но могли видеть, насколько плохо это выглядело бы. Например, они использовали кусок фольги вместо голограммы, и он не давал трёхмерного изображения».

Топ-10 загрузок пиратских BBS

1. Windows 3.1 (Microsoft)
2. Excel 4.0 (Microsoft)
3. Norton Utilities 6.0 (Symantec)
4. WordPerfect for Windows 5.1 (WordPerfect)
5. Stacker 2.0 (Stac Electronics)
6. AutoMap (AutoMap)
7. Procomm Plus 2.0 (Datastorm Technologies)
8. PC Tools Deluxe 7.1 (Central Point Software)
9. QEMM-386 6.0 (Quarterdeck Office Systems)
10. WordPerfect 5.1 (WordPerfect)

Выглядит знакомо. Это очень близко к недавнему списку топ-10 легальных программ. Неудивительно, поскольку популярные программы также чаще всего и воруются.

Приведённый выше список был составлен по результатам опроса пиратских BBS с помощью Джона Рэкхема. Он объясняет, что активность настолько высока, что профиль меняется из недели в неделю, а игры являются наиболее переменчивыми позициями (вот почему их невозможно отследить). Поскольку соглашений о неразглашении в пиратском мире не существует, а обмен бета-копиями программного обеспечения — пиратская традиция, Windows 3.1 заняла сильную позицию ещё до официального выхода. Кстати, к OS/2 2.0 проявляется лишь поверхностный интерес — это зловещая новость для IBM, если пиратский интерес хоть сколько-нибудь служит индикатором продаж.

Ассоциация издателей программного обеспечения: нацисты или программная полиция?

Расследование Rambone

Ассоциация издателей программного обеспечения (SPA) является основной торговой ассоциацией отрасли программного обеспечения для микрокомпьютеров. Основанная в 1984 году 25 фирмами, SPA сегодня насчитывает более 750 членов, в том числе крупные компании делового, потребительского и образовательного сегментов, а также небольшие фирмы с годовым доходом менее $1 миллиона. SPA стремится продвигать отрасль и защищать интересы своих членов.

SPA имеет две категории членства: полное и ассоциированное. Программные фирмы, производящие, выпускающие, разрабатывающие или лицензирующие программное обеспечение для микрокомпьютеров и несущие основную ответственность за его маркетинг и продажи, имеют право подать заявку на полное членство. Фирмы, разрабатывающие, но не публикующие программное обеспечение, также имеют на это право. Ассоциированное членство открыто для фирм, не публикующих программное обеспечение, но оказывающих услуги программным компаниям. В их числе — поставщики, консультанты, компании по маркетинговым исследованиям, дистрибьюторы и производители оборудования.

Лоббирование

SPA представляет интересы отрасли перед Конгрессом США и исполнительной ветвью власти и держит членов в курсе событий в Вашингтоне, О.К., которые на них влияют. Борьба с пиратством программного обеспечения входит в число её главных приоритетов. SPA является основной защитой отрасли от нарушителей авторских прав на программное обеспечение как в Соединённых Штатах, так и за рубежом. Судебные разбирательства и непрерывные рекламные кампании — это способы, с помощью которых SPA стремится защищать авторские права своих членов.

Таков образ, который SPA хочет создать у широкой публики, и в целом у меня нет возражений. В ходе продолжительной беседы с Терри Чайлдс из SPA я узнал несколько вещей. Главный источник информации ассоциации — их горячая линия, и звонки обычно поступают от недовольных сотрудников, мечтающих поквитаться с бывшими начальниками. Пример тому — компания, купившая одну копию Microsoft Works, при том что более 100 сотрудников, судя по всему, пользовались одной и той же копией. Одна конкретная секретарша была уволена — по какой причине, не знаю, — так что она позвонила в программную полицию SPA и всё выложила. Как только это произошло, SPA запустила механизм, поручив Федеральным маршалам получить ордер и ворваться в здание, как к себе домой. С помощью хитрой программки, которая ищет на машинах нелегальные копии программного обеспечения, они обнаружили программы, не зарегистрированные на данных машинах. Бам! — поймали, как дохлую крысу в клетке. SPA отказалась комментировать, что произошло с этой компанией после обыска, но сказала, что компания была оштрафована на «X» долларов за каждую нелегальную копию.

Миссис Чайлдс оказалась весьма полезной: она объяснила идею, стоящую за ассоциацией, и то, что они отстаивают. Я был весьма впечатлён тем, что она рассказала. Однако когда я поднял вопрос о деле Davy Jones Locker, она сообщила, что не уполномочена отвечать на вопросы, касающиеся этого дела, и направила меня к Элейн Розентал. Несколько часов спустя я позвонил ей, и поначалу она, казалось, была весьма полезной, но затем решила перевести меня на громкую связь с основателем ассоциации Кеном Уошем.

С самого начала я понял, что прямого ответа от него не получу. Первый вопрос, который я задал, — не получил ли кто-то, не входящий в SPA, аккаунт для входа на DJL и не передал ли его им вместе с логами BBS. Прямого ответа он не дал — только то, что SPA удалось получить информацию. Затем я спросил, какие меры принимаются в отношении DJL, и снова получил уклончивый ответ.

Наконец, я спросил, какой штраф, вероятно, будет наложен в этом деле. Он отказался отвечать.

Но из всего этого я узнал один весьма интересный факт. Деньги, полученные по этому и подобным делам, не идут компаниям-разработчикам программного обеспечения, которые SPA якобы

защищает. Вместо этого они поступают прямо в казну самой SPA! Видимо, они сами не прочь попробовать эти Mercedes.

И вот ещё несколько интересных подробностей о SPA. Мало того что они штрафуют компании за нелегальное программное обеспечение и кладут деньги в карман, так ещё и ежегодный членский взнос для компаний-разработчиков может составлять от $700 до $100 000! Мне кажется, что бороться с пиратством куда выгоднее, чем им заниматься.

Тем, кто сейчас управляет или думает об управлении пиратской доской, я бы посоветовал не брать плату за доступ. Даже если вы утверждаете, что деньги идут только на обновление оборудования, в конечном счёте, если вас поймают, собранные деньги станут доказательством того, что вы продавали защищённое авторским правом программное обеспечение ради финансовой выгоды.

Кошмар с бэкдором в Vision-X

Автор: Rambone

В пиратском мире, похоже, существует заблуждение о неуязвимости любого BBS-программного обеспечения. Однако около месяца назад несколько участников команды Oblivion разобрали .93 (номер версии Vision-X) и нашли бэкдоры. Неприятность состоит в том, что команда V-X поместила эти бэкдоры, чтобы отследить, с какого бета-сайта утекают бета-копии. Что ж, они нашли бэкдоры и позвонили на несколько бордов и воспользовались ими.

1. История от людей, которые взломали борды, такова: один из двух участников был разъярён, потому что написал регистрационный код для .93, позволявший любому запускать его независимо от оплаты. Когда команда V-X узнала об этом, они занесли его в чёрный список, лишив возможности входить на любую V-X систему. Это было зашито в код намертво, так что ни один сисоп не мог впустить его под этим никнеймом. В общем, история такова: они проникли на несколько BBS и даже выходили в DOS, чтобы осмотреться, но не имели намерений уничтожать данные. По сути, они хотели выявить слабые места программного обеспечения. Проблема началась, когда они опубликовали бэкдоры в национальной сети — а это значит, что теперь любой ламер мог воспользоваться этим бэкдором в своих целях. По словам ребят из Oblivion, они данные не уничтожали, но некоторые ламеры, увидевшие бэкдоры в сети, — уничтожали. Они сожалеют о публикации бэкдоров. Они не осознавали, что есть люди, достаточно злобные, чтобы уничтожать данные.

2. Команда Vision-X уверена, что именно команда Oblivion положила борды — некоторые говорят, что те даже сами признались в этом. В этих историях есть серьёзное противоречие, и на данный момент непохоже, что кто-либо когда-нибудь узнает всю правду о произошедшем.

Бэкдоры никогда не были хорошей идеей, даже если авторы были уверены, что их никогда не найдут. Недавняя волна сбоев систем доказывает, что бэкдоры в конечном счёте будут обнаружены. С другой стороны, даже если бэкдоры в BBS-программном обеспечении найдены, их следует оставить для использования по первоначальному назначению. Большинство авторов, встраивающих бэкдоры в системы, делают это для защиты своих инвестиций и тяжёлого труда. Большинство BBS-программистов в наши дни работают над программным обеспечением на благо сообщества пользователей модемов и рассчитывают на небольшое денежное вознаграждение за свой труд. Сисопам использовать его без разрешения — неправильно. Хватит жмотиться, поддержите программное обеспечение, от которого сами же ждёте поддержки. Какой смысл запускать взломанное ПО, если нельзя получить поддержку от авторов и не попасть в их сеть. Небольшая сумма, о которой идёт речь, — это хорошая инвестиция в будущее вашей борды.

Журнал «BAD» оправдывает своё название

Автор: Rambone

Я никогда не читал Bad Magazine до недавнего времени. Везде, где о нём заходил разговор, я видел лишь комментарии о том, что это трата места на жёстком диске. Однако когда вышел восьмой номер Bad, я услышал, что там было несколько пренебрежительных замечаний обо мне и куча другой беспочвенной информации.

Так что я взял и прочитал его — и обнаружил одну ложь за другой. Никогда не видел такого насквозь лживого журнала, как BAD №8. Похоже, они решили, что я упомянул их в журнале Phrack: «Bad Magazine получил своё первое упоминание в журнале Phrack». Смешно то, что единственное упоминание BAD Magazine в Phrack до этого момента — это замечание, приписанное The Grim Reaper, которое я перепечатал.

Мне плевать на столь жалкий и унылый журнал, как BAD, и я никогда не упоминал его и не собирался — пока они сами не подняли тему, выпустив в меня шпильку.

«Ребята из Phrack, однако, не сделали домашнюю работу, когда упомянули об этом». Это цитата из BAD о комментариях, касающихся Vision-X, хотя статья была вовсе не об этом. Чего они не знают: перед тем как опубликовать что-либо в Phrack о задержании The Grim Reaper, я лично позвонил ему и поговорил с ним. Именно об этом и была статья, а не о каком-то унылом журнале под названием BAD и о том, что они сделали. Они возложили на меня ответственность за неподкреплённые факты, тогда как на самом деле я все их проверил. Комментарии Grim Reaper о Vision-X не были моей заботой — меня интересовал его арест за мошенничество с кредитными картами. Замечания о BAD были сделаны TGR, так что похоже, что «ребята из BAD» не сделали СВОЮ домашнюю работу!

«Rambone, очевидно, не слишком хорошо знаком с пиратским миром». Ещё одно нелепое и необоснованное замечание. Ребята, вы точно не сделали домашнюю работу — лучше бы порасспросили побольше, прежде чем делать безответственные обвинения. Последнее, что я скажу об этом: когда люди собирают журнал, им следует искать авторов, которые расследуют факты, а не выдумывают их. Если бы они на самом деле прочитали мою статью, они бы знали, что я не сказал о их журнале ни слова, а лишь процитировал The Grim Reaper. С такими авторами, как в BAD, я не советовал бы никому тратить время на его чтение — разве что если вы любите таблоиды вроде National Inquirer, хотя хотя бы там некоторые статьи имеют фактическое основание.

Игры

Игра месяца: Links 386 Pro

-*- Информация о релизе -*-		-*- Информация об игре -*-	
Крэкер	Нет	Издатель	MICROPLAY
Тип защиты	Нет	Графика	Мин. SVGA
Поставщик	The Witch King	Звук	Любой
Дата релиза	07/13/92	Оценка [1-10]	10

Прошу прощения за то, что перепечатываю информационный файл, но я немного поленился.

С появлением Super VGA мониторов и снижением цен на них компании начинают выпускать специальные игры, использующие преимущества режима SVGA. Большинство этих игр

по-прежнему будут работать в режиме VGA, так что не расстраивайтесь.

Одна из последних на сегодняшний день — и, пожалуй, лучшая — это Links 386 Pro, что, как следует из названия, требует как минимум 386-го процессора. Установка игры — одна из наиболее впечатляющих, которые я когда-либо видел: она охватывает каждый аспект вашего оборудования, чтобы использовать его по максимуму. Один из трудноперевариваемых моментов — необходимость иметь не менее 512 кБ памяти на видеокарте, соответствующей стандарту VESA. Если карта ему соответствует, установщик достаточно умён, чтобы попытаться найти её самостоятельно.

Сама игра является значительным улучшением по сравнению с предшественницей — Links. Графика заметно улучшена (что само по себе достижение), добавлено множество опций и исправлены ошибки. Компания также прислушалась к клиентам и добавила многие предложенные ими новые функции.

При первой загрузке 386 Pro вас встречает вид поля для гольфа сзади, а не скучный пустой экран оригинала. Оттуда можно настроить практически всё что угодно: выбор клюшки, состояние фарватера и текстуру гринов. Можно даже выбрать условия ветра. Одна из наиболее впечатляющих функций помимо превосходной графики — возможность держать открытыми несколько окон во время игры.

Допустим, вы на первой лунке и готовитесь к удару по фарватеру — если вы можете туда добраться, одновременно можно открыть другое окно с видом на фарватер, ожидая, куда упадёт мяч. Это лишь одно из многих доступных окон, которых можно открыть до четырёх одновременно. Впрочем, поиграв достаточно долго, я бы рекомендовал ограничиться одним-двумя.

Если вы размышляете над покупкой игры, которая использует все возможности вашего SVGA монитора, — не ищите дальше: Links 386 Pro. Это волна будущего, и она уже здесь.

Больше не покупай консольные игры — копируй их

Особая благодарность Snow Dog

Ниже — информационный фрагмент о GameDoctor. Грубо говоря, вы можете купить устройство под названием GameDoctor, подключить его к своему ПК и скопировать данные ROM на жёсткий диск в сжатом формате. Оттуда их можно отправить по сети, через модем или отнести к другу. Подключите GameDoctor к ПК, подключите консольную игру к GameDoctor и перенесите сжатый файл данных на чистый картридж. Вот так — мгновенный Super Mario Brothers. В следующем номере будет более подробный обзор этого устройства, а пока — небольшой предварительный обзор.

Snow Dog пишет:

Устройства — внешние SCSI-интерфейсы, примерно размером с Super NES, но шире, приспособленные для японских (Super Famicom) картриджей. Их производит Electronics Nippon, известная в Штатах как NEC, и у друга есть одно такое, которое работает и на его Amiga 2000, и на его 486-33 (SCSI универсален).

В комплекте идут пять дисков с Famicom OS, которую можно использовать на логическом разделе жёсткого диска размером около шести мегабайт — поскольку игры SNES измеряются в мегабитах и НИКОГДА не превысят четырёх мегабайт или около того, но OS нужно место. Контроллеры и прочее подключаются к копировальным устройствам.

Если вы извлечёте картридж SNES или Genesis из корпуса и поместите в корпус SF, их тоже можно скопировать. Это работает как teledisk, а Altered Reality по номеру (303)443-1524 поддерживает файлы консольных игр. Всё, что нужно — скачать и использовать собственный консольный копировальщик для записи на картридж, или, по желанию, если это игра SNES или Famicom, играть прямо с OS. Игры Genesis в OS SF не работают, поэтому их нужно копировать на картридж.

Существуют японские копировальщики специально для Mega Drive (Genesis), которые делают то же самое, за исключением того, что OS специфична для Sega и вам придётся копировать игры SNES. Есть также копировальщик для NEC PC Engine (Turbo Graphics и Super Graphics), поскольку они сами сделали эту систему, но он является проприетарным и работает только с форматом Turbo.

Я никогда не видел и не работал с внутренней моделью, но во внутренней модели 5,25" полной высоты она есть в каталоге NEC... Я заказал каталог, увидев рекламу в Electronic Gaming Monthly, а довольно состоятельный друг взял и купил систему. Он также купил японский Street Fighter II за $130 и скопировал его для всех нас. Какая щедрость! Конечно, нам пришлось купить картриджи и заплатить ему по $20, но он заработал $100 прибыли. Хорошая сделка для него!

Вот и всё на сегодня. Привет Cool Hand, Ford Perfect, Lestat, RifleMan, The CrackSmith, AfterMath, обоим Night Rangers, Kim Clancy, Bar Manager, Butcher, Venom и всем курьерам, которые помогают всему работать.

Особая благодарность Tempus за убойное ANSI!

До следующего раза — не прекращайте играть.

Сотовая телефония. Часть II

Автор: Brian Oblivion

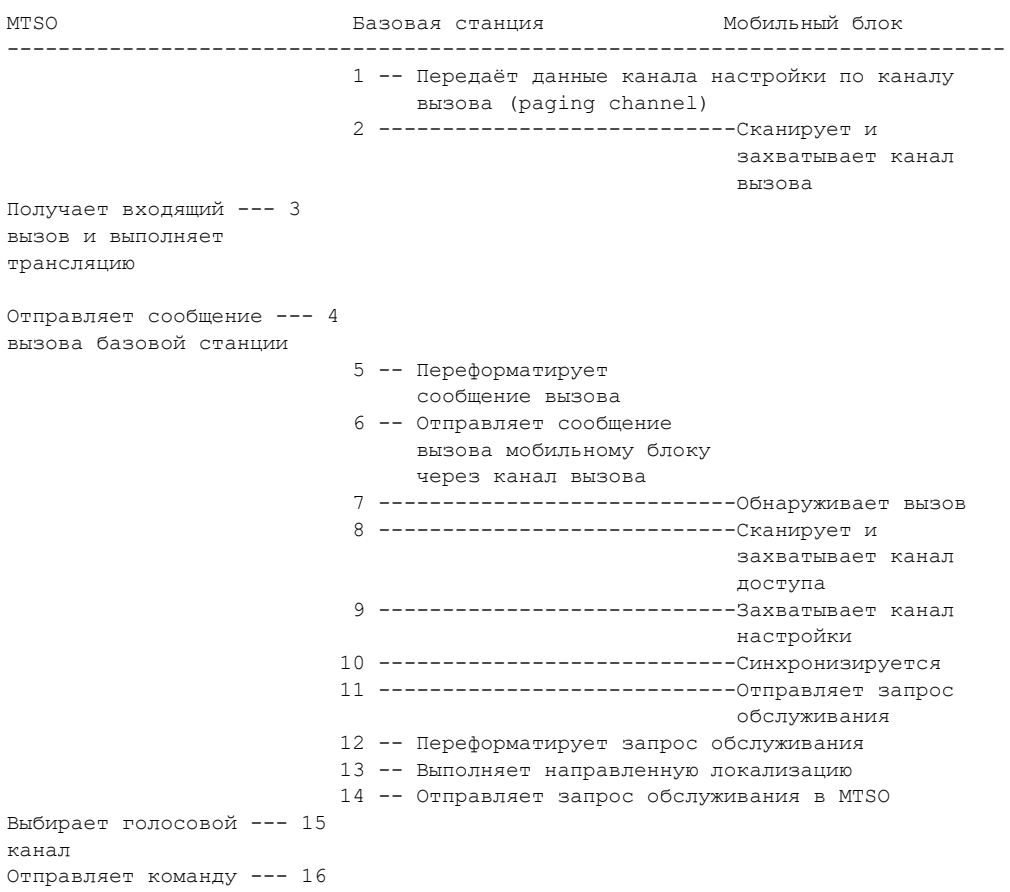
При поддержке: Restricted-Data-Transmissions (RDT)
"Truth Is Cheap, But Information Costs."

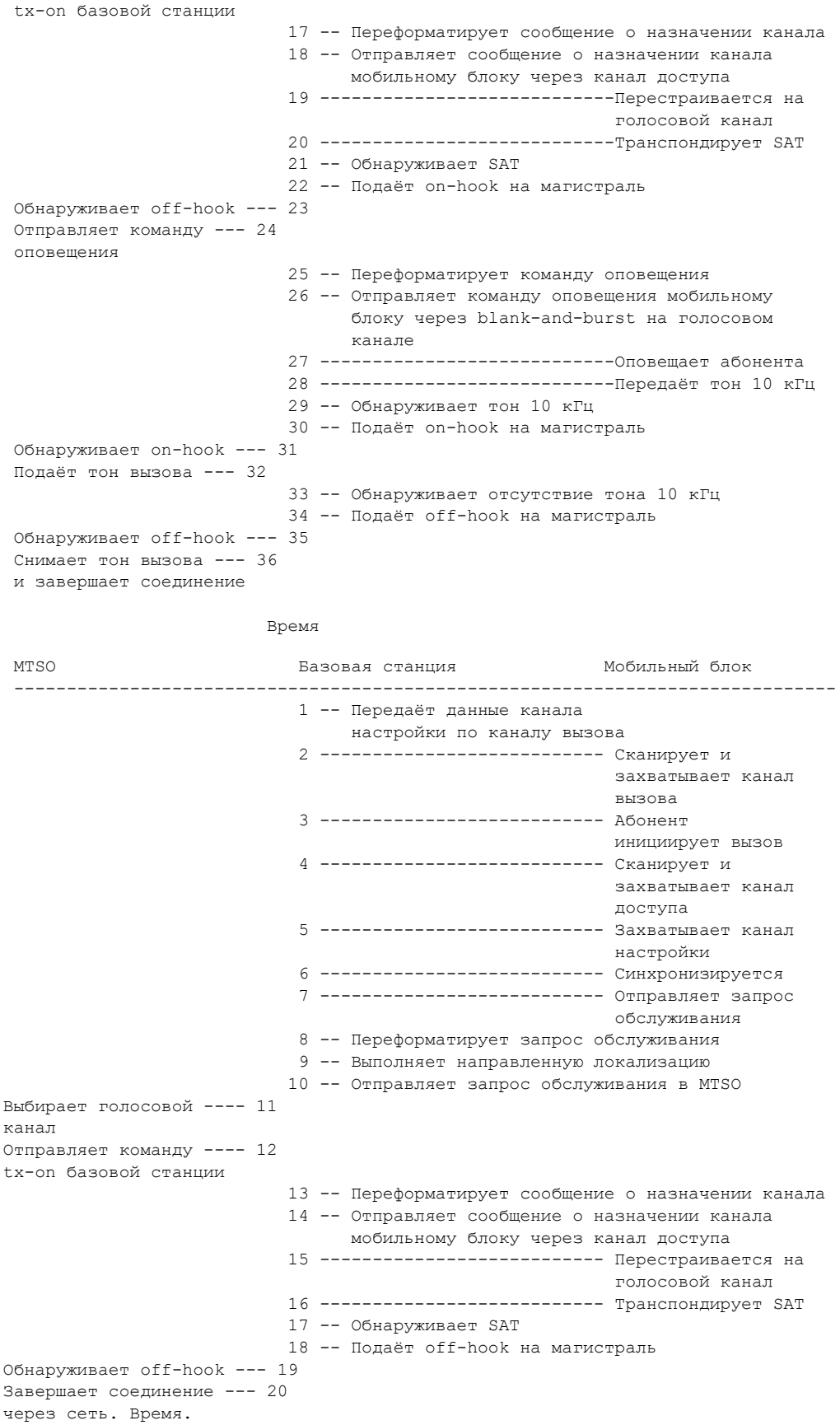
1 июня 1992 г.

В Phrack №38 я рассмотрел историю сотовой телефонии, методы мониторинга и краткое описание систем-предшественников. В части II я опишу последовательности обработки вызовов для звонков, инициированных со стороны фиксированной сети и со стороны мобильного абонента, а также форматы сигнализации для этих процессов. Прошу извинить за объём материала, однако я считаю его важным для всех, кто интересуется принципами работы сети. Имейте в виду, что добавить что-то существенное к столь конкретной теме практически невозможно, и большая часть текста взята дословно из отраслевых стандартов с моими комментариями и дополнениями, рассыпанными по всему тексту.

Последовательности обработки вызовов

Последовательность обработки вызова, инициированного со стороны фиксированной сети





Давайте повторим распределение частот для проводных (Wireline) и беспроводных (non-Wireline) систем. Напомним, что проводное обслуживание обычно предоставляется местной телефонной компанией — в моём регионе это NYNEX. Беспроводные компании, как правило, работают под управлением сторонних операторов; в моём регионе это Cellular One (принадлежащая Southwestern

Bell). Каждая компания занимает свой участок электромагнитного спектра. Покрытие не является сплошным: следует помнить, что в этом же диапазоне работают и транкинговые бизнес-системы 800 МГц. Голосовые каналы расположены через каждые 30 кГц, канналы данных — через 10 кГц.

```
Диапазон частот         Использование
-----------------------------------------------------------------
870.000 - 879.360       Cellular One (вход с мобильного 825.000 - 834.360)
880.650 - 890.000       NYNEX (вход с мобильного 835.650 - 845.500)
890.000 - 891.500       Cellular One (вход с мобильного 845.000 - 846.500)
891.500 - 894.000       NYNEX (вход с мобильного 846.500 - 849.000)
879.390 - 879.990       Cellular One (данные)
880.020 - 880.620       NYNEX (данные)
```

Потоки данных кодируются в формате NRZ (Non-return-to-zero): логические единицы и нули представлены переходами с нуля в единицу и с единицы в ноль соответственно. Это необходимо для того, чтобы широкополосные данные могли модулировать передатчик посредством двоичной частотной манипуляции (BFSK); при этом единицы и нули, поступающие на модулятор, ДОЛЖНЫ соответствовать номинальным пиковым девиациям частоты ±8 кГц относительно несущей частоты.

Сборка воедино: сигнализация на управляющих каналах

Следующая информация окажется бесценной для любителей, перехватывающих сигналы сотовых телефонов с помощью сканера и имеющих доступ к сигналам управляющего канала. Все приведённые ниже сведения соответствуют стандартам EIA/TIA — FCC. Между сотовыми телефонами существует множество различий, однако все они должны взаимодействовать с мобильной сетью и понимать друг друга, а также базовые станции. Поэтому методы обработки вызовов и цифровой сигнализации единообразны во всей отрасли.

Обработка мобильных вызовов

Исходящий вызов

Изначально наземная станция передаёт первую часть своего SID на мобильный, прослушивающий некоторый управляющий канал, затем — количество каналов вызова, запрос ESN и статус регистрации мобильного, который может принимать значение 0 или 1. Если регистрация установлена в единицу, мобильный передаёт как MIN1, так и MIN2 при доступе к системе; ещё один бит «1» указывает на прерывистую передачу (DTX); бит чтения управляющего заполнителя (RCF) должен быть установлен в 1; функции доступа (если они совмещены с операциями вызова) требуют установки поля в 1, в противном случае CPA (combined paging access — совмещённый вызов и доступ) обнуляется.

Входящий вызов

Входя в задачу сканирования выделенных управляющих каналов (Scan Dedicated Control Channels Task), мобильный должен измерить уровни сигнала каждого выделенного управляющего канала, назначенного системе A (если она включена). В противном случае проверяются управляющие каналы системы B. Значения, заданные в параметре NAWC (Number of Additional Words Coming) в поезде сообщений системных параметров, сообщают мобильному, была ли получена вся

предназначенная информация. Поле EDN используется для перекрёстной проверки; сообщения управляющего заполнителя не учитываются при подсчёте NAWC. Если получен правильный код BCH вместе с нераспознанным сообщением служебных параметров, оно должно учитываться в счётчике NAWC, однако соответствующий блок не должен пытаться выполнить инструкции.

При нормальных условиях мобильные должны настроиться на наиболее мощный выделенный управляющий канал, принять передачу системных параметров и в течение 3 секунд выполнить следующее:

• Установить 14 наиболее значимых бит SID в значение поля SID1.
• Установить младший бит SID в 1, если статус обслуживающей системы включён, или в 0 — если нет.
• Установить число каналов вызова N равным 1 плюс значение поля N-1.
• Установить канал вызова FIRSTCHP следующим образом:
• Если SIDs = SIDp, то FIRSTCHPs = FIRSTCHPp (11-битный канал вызова).
• Если SIDs = SIDp и обслуживающая система включена, установить FIRSTCHPs на начальный выделенный канал системы B.
• Если SIDs = SIDp и обслуживающая система отключена, установить FIRSTCHPs на первый выделенный управляющий канал системы B.
• Установить LASTCHPs равным FIRSTCHPs + Ns - 1.
• Если мобильный оснащён поддержкой автономной регистрации, он должен:
• Установить шаг регистрации (REGINCRs) в значение по умолчанию — 450.
• Установить статус идентификатора регистрации в состояние «включён».

Знаю, что всё это звучит несколько загадочно, — но такова специфика спецификаций. Данные есть данные, украсить их невозможно. После этого мобильный должен приступить к задаче выбора канала вызова (Paging Channel Selection Task). Если завершить её на наиболее мощном выделенном канале не удаётся, может быть использован второй по мощности выделенный канал, и трёхсекундный интервал начинается заново. Неполный результат должен привести к проверке статуса обслуживающей системы и смене состояния включено/выключено, что позволяет мобильному снова приступить к задаче сканирования выделенных управляющих каналов.

Операторам разрешено передавать инструкции для мобильных в своих локальных системах, включая роуминговых абонентов, домашние системы которых входят в состав группы. Может быть передан новый канал доступа с полем нового канала доступа, установленным на начальный канал доступа. Автономно зарегистрированные мобильные могут увеличивать следующий зарегистрированный идентификатор на некоторое фиксированное значение, однако поле REGINCR глобального сообщения о действии должно быть соответствующим образом установлено. Кроме того, для того чтобы все мобильные вошли в задачу инициализации и просканировали выделенные управляющие каналы, должно быть передано глобальное сообщение RESCAN.

Прежде чем получить доступ к какой-либо системе через обратный управляющий канал, мобильным станциям может потребоваться прочитать сообщение управляющего заполнителя.

Доступ к системе для мобильных передаётся по прямому управляющему каналу следующим образом. Цифровой цветовой код (DCC), идентифицирующий наземную станцию, передаётся в служебном сообщении системных параметров; поля классов перегрузки установлены в ноль у ограниченной части, остальные — в 1. Параметры доступа «занято-свободно» (BIS) обнуляются, когда мобильным запрещено проверять обратный управляющий канал, и сообщение должно быть добавлено в служебные данные. Когда мобильные не могут использовать обратный управляющий канал для попыток передачи сигнала захвата или занятости, параметры попыток доступа также должны быть включены в служебные данные. Когда наземная станция получает преамбулу захвата, совпадающую с её цифровым цветовым кодом с 1 ошибкой в бите или без ошибок, биты «занято-свободно» на прямом управляющем канале должны быть установлены в состояние

«занято» в течение 1,2 миллисекунды с момента последнего бита захвата. Затем бит «занято-свободно» должен оставаться в состоянии «занято» не менее 30 мс после последнего бита последнего слова принятого сообщения, либо до истечения суммарного времени в 175 мс.

Подтверждение канала

Мобильные должны отслеживать управляющие сообщения станции и отвечать как на звуковые, так и на локальные управляющие команды, даже если наземная станция не обязана отвечать. Биты MIN должны совпадать. После этого выполняется вход в задачу доступа к системе с ответом на вызов, как описано выше, и запускается таймер доступа.

Время работы таймера:

• 12 секунд для исходящего вызова
• 6 секунд для ответа на вызов
• 6 секунд для ответа на команду
• 6 секунд для регистрации

Затем код последней попытки устанавливается в ноль, и оборудование приступает к задаче сканирования каналов доступа (Scan Access Channels Task), чтобы найти два канала с наибольшим уровнем сигнала, на которые оно настраивается, и входит в задачу получения параметров попыток доступа (Retrieve Access Attempts Parameters Task).

На этом этапе максимальное число попыток захвата и число занятых сигналов устанавливаются по 10. Затем проверяется бит чтения управляющего заполнителя (RCF): если RCF равен нулю, мобильный читает сообщение управляющего заполнителя, устанавливает DCC и WFOM (ожидание поезда служебных сообщений перед доступом к обратному управляющему каналу) в соответствующие поля и устанавливает соответствующий уровень мощности. Если ни поле DCC, ни сообщение управляющего заполнителя не получены, а время доступа истекло, мобильная станция переходит к задаче определения обслуживающей системы (Serving System Determination Task). Но если время доступа ещё не истекло, мобильная станция входит в задачу альтернативного канала доступа (Alternate Access Channel Task). Затем BIS устанавливается в 1, и проверяется бит WFOM. Если WFOM равен 1, станция входит в задачу обновления служебной информации (Update Overhead Information Task); если WFOM равен 0, требуется случайная задержка от 0 до 200 мс, ±1 мс. После этого станция входит в задачу захвата обратного управляющего канала (Seize Reverse Control Channel Task).

Далее следует запрос обслуживания. Эта задача требует, чтобы мобильный продолжал отправлять своё сообщение наземной станции согласно следующим инструкциям:

• Слово A требуется всегда.
• Слово B должно быть отправлено, если код последней попытки LT равен 1, или если E требует MIN1 и/или MIN2 и статус ROAM отключён, или если станция была вызвана двухсловным управляющим сообщением.
• Слово C передаётся с S (серийным номером) равным 1.
• Слово D требуется, если доступ является исходящим вызовом.
• Слово E передаётся, когда доступ является исходящим вызовом и набрано от 9 до 16 цифр. После того как мобильный передал полное сообщение, перед выключением несущей необходимо ещё 25 миллисекунд немодулированной несущей. После отправки слов с A по E следующая задача мобильного зависит от типа доступа.

Подтверждение команды требует входа в задачу определения обслуживающей системы (Serving System Determination Task).

• Исходящий вызов означает вход в задачу ожидания сообщения (Await Message Task).

• Ответ на вызов — то же, что и исходящий вызов.

Регистрация требует ожидания подтверждения регистрации (Await Registration Confirmation), которое должно быть завершено в течение 5 секунд — иначе фиксируется сбой регистрации. То же самое верно для задачи ожидания сообщения: незавершённая задача через 5 секунд отправляет мобильный в задачу определения обслуживающей системы. При исходящем вызове или ответе на вызов мобильный обновляет параметры, полученные в сообщении. Если R равно 1, мобильный входит в задачу автономной регистрации (Autonomous Registration Task), в противном случае — в задачу подтверждения начального голосового канала (Initial Voice Channel Confirmation Task). Доступ при исходящем вызове может быть перехватом или переадресацией: в этих случаях мобильные входят в задачу определения обслуживающей системы. То же верно для ответа на вызов. Но если доступ является исходящим вызовом и пользователь завершает его во время этой задачи, вызов должен быть освобождён через голосовой канал, а не через управляющий.

Если мобильная станция оснащена поддержкой направленного повтора (Directed Retry) и новое сообщение получено до того, как все четыре слова сообщения направленного повтора переданы, она должна перейти в задачу определения обслуживающей системы. Там код последней попытки (LT) должен быть установлен согласно полю ORDQ (квалификатор команды) сообщения следующим образом:

```
Если 000,  LT устанавливается в 0
Если 0001, LT устанавливается в 1
```

После этого мобильный очищает список управляющих каналов для сканирования при обработке направленного повтора (CCLIST) и проверяет каждое поле CHANPOS (позиция канала), содержащееся в словах три и четыре сообщения. Для ненулевых полей CHANPOS мобильный вычисляет соответствующий номер канала, прибавив CHANPOS к FIRSTCHA минус один. После этого мобильный должен определить, находится ли каждый номер канала в наборе, предназначенном для сотовых систем. При положительном ответе этот/эти канал(ы) добавляются в CCLIST.

Ожидание ответа

Здесь устанавливается таймер оповещения на 65 секунд (от 0 до +20 процентов). В течение этого периода могут происходить следующие события:

• Если время истекает, мобильный отключает передатчик и входит в задачу определения обслуживающей системы.
• Ответ требует отключения тонового сигнала и входа в задачу разговора (Conversation Task).
• Если любое из перечисленных ниже сообщений получено в течение 100 миллисекунд, мобильный должен сравнить цифры SCC, идентифицирующие сохранённые и корректные частоты SAT для станции, с PSCC (текущим цветовым кодом SAT). Если они не совпадают, команда игнорируется. Если совпадают, для каждой команды выполняются следующие действия:

Хэндовер: тоновый сигнал гасится на 500 мс, тон выключается, передатчик выключается, уровень мощности регулируется, производится настройка на новый канал, устанавливаются новый SAT и новое поле SCC, передатчик включается, таймер угасания сбрасывается, тоновый сигнал включается. Ожидание ответа.

Оповещение: сброс таймера оповещения на 65 секунд; оставаться в задаче ожидания ответа.

Остановить оповещение: погасить тоновый сигнал и войти в задачу ожидания команды (Waiting for Order Task).

Освобождение: тоновый сигнал выключается, ожидание 500 мс, затем вход в задачу освобождения (Release Task).

Аудит: отправить подтверждение наземной станции; оставаться в задаче ожидания ответа.

Обслуживание: сброс таймера оповещения на 65 секунд; оставаться в задаче ожидания ответа.

Изменить мощность: отрегулировать передатчик до требуемого уровня мощности и отправить подтверждение наземной станции; оставаться в задаче ожидания ответа.

Локальное управление: если локальное управление включено и получена соответствующая команда, проверить поле LC и определить действие.

Все прочие команды данного типа игнорируются.

Разговор

В этом режиме таймер задержки освобождения устанавливается на 500 мс. Если завершение включено, мобильный устанавливает статус завершения в «отключено» и ждёт 500 мс перед входом в задачу освобождения. Затем могут выполняться следующие действия:

• При завершении вызова необходимо проверить таймер задержки освобождения. Если время истекло, выполняется вход в задачу освобождения; если нет — мобильный ждёт истечения и затем входит в задачу освобождения.
• При запрошенном пользователем флэш-сигнале тоновый сигнал включается на 400 мс. Если в течение этого интервала получен корректный тон команды, флэш немедленно прерывается и команда обрабатывается. Флэш в таком случае считается недействительным.
• При получении перечисленных ниже команд в течение 100 мс мобильный должен сравнить SCC с PSCC; если они не совпадают, команда игнорируется. Если совпадают, возможны следующие действия:

Хэндовер: тоновый сигнал включается на 50 мс, затем выключается, передатчик выключается, уровень мощности регулируется, производится настройка на новый канал, устанавливается новый SAT, SCC принимает значение поля SCC из сообщения, передатчик включается, таймер угасания сбрасывается; оставаться в задаче разговора.

Отправить адрес вызываемого: при получении в течение 10 секунд после последнего корректного флэш-сигнала адрес вызываемого отправляется наземной станции. Мобильный остаётся в задаче разговора. В противном случае также оставаться в задаче разговора.

Оповещение: включить тоновый сигнал, ждать 500 мс, затем войти в задачу ожидания ответа.

Освобождение: проверить таймер задержки освобождения. Если время истекло, мобильный входит в задачу освобождения; если нет — ждёт и входит в задачу освобождения по истечении времени.

Аудит: подтверждение команды отправляется наземной станции; оставаться в задаче разговора.

Обслуживание: тоновый сигнал включается, ожидание 500 мс, затем вход в задачу ожидания ответа.

Изменить мощность: отрегулировать передатчик до уровня мощности, заданного кодом квалификатора команды, и отправить подтверждение наземной станции; оставаться в задаче разговора.

Локальное управление: если локальное управление включено и получена соответствующая команда, поле LC проверяется для последующего действия и подтверждения.

Все прочие команды данного типа игнорируются.

Освобождение

В режиме освобождения необходимо выполнить следующие шаги:

• Тоновый сигнал передаётся в течение 1,8 с. Если в момент начала тонового сигнала шёл флэш-сигнал, его необходимо продолжить так, чтобы действие завершилось в течение 1,8 с.
• Остановить тоновый сигнал.
• Выключить передатчик.
• Мобильная станция входит в задачу определения обслуживающей системы.

Выше изложена спецификация совместимости мобильной/наземной станции сотовой системы. Далее следуют форматы сигнализации, также взятые из указанного документа. Я вручную перевёл все эти таблицы в ASCII, так что цените их — это было непросто. Зато теперь я определённо понимаю весь формат работы сотовой связи в целом.

Форматы сигнализации

Существует два типа непрерывных широкополосных потоков данных. Первый — прямой управляющий канал (Forward Control Channel, FOCC) — передаётся от наземной станции к мобильной. Второй — обратный управляющий канал (Reverse Control Channel, RECC) — передаётся от мобильной к наземной станции. Каждый поток данных работает на скорости 10 кбит/с, ±1 бит/с. Форматы каждого из каналов приведены ниже.

Прямой управляющий канал (Forward Control Channel)

Прямой управляющий канал состоит из трёх отдельных информационных потоков: поток A, поток B и поток «занято-свободно» (busy-idle). Все три потока мультиплексируются вместе. Сообщения для мобильных станций, у которых младший бит номера MIN равен «0», передаются в потоке A, а с «1» — в потоке B.

Поток «занято-свободно» содержит биты занято-свободно, которые указывают на состояние обратного управляющего канала. Если бит занято-свободно равен «0», обратный управляющий канал занят; если «1» — свободен. Бит занято-свободно расположен в начале каждой последовательности точек (dotting sequence), последовательности синхронизации слова (word sync sequence), в начале первого повтора слова A, а также после каждых 10 бит сообщения.

Синхронизация мобильных станций с входящими данными достигается посредством 10-битной последовательности точек (1010101010) и 11-битной последовательности синхронизации слова (11100010010). Каждое слово содержит 40 бит, включая биты чётности, и повторяется 5 раз, после чего именуется «блоком». В многословном сообщении второй и последующие блоки слов формируются так же, как и первый, включая последовательности точек и синхронизации. «Слово» формируется, когда 28 информационных бит кодируются в (40, 28; 5) код BCH (Боуза–Чоудхури–Хоквенгема). Крайний левый бит считается наиболее значимым.

Порождающий полином для кода (40, 28; 5) BCH:

$$G_B(X) = X^{12} + X^{10} + X^8 + X^5 + X^4 + X^3 + X^0$$

Каждое сообщение FOCC может состоять из одного или нескольких слов. Сообщения, передаваемые по прямому управляющему каналу:

• Управляющее сообщение для мобильной станции
• Служебное сообщение
• Сообщение управляющего заполнителя

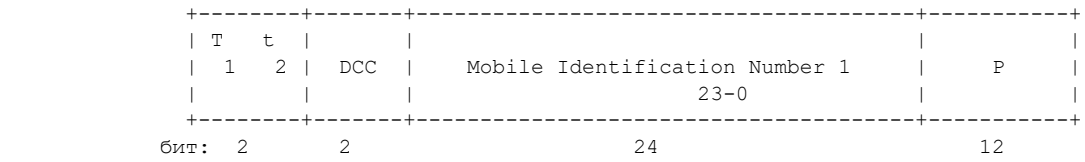
Сообщения управляющего заполнителя могут вставляться между сообщениями и между блоками слов многословного сообщения.

Форматы сообщений: передаются в потоке A или B.

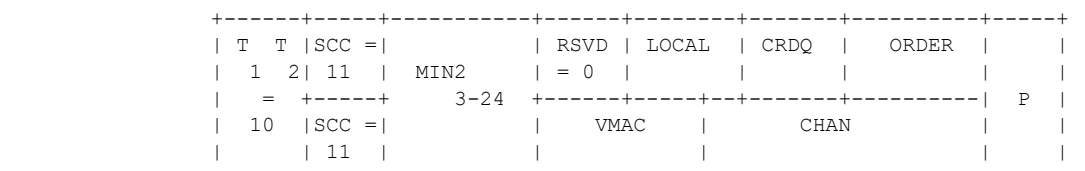
Управляющее сообщение для мобильной станции

Управляющее сообщение для мобильной станции может состоять из одного, двух или четырёх слов.

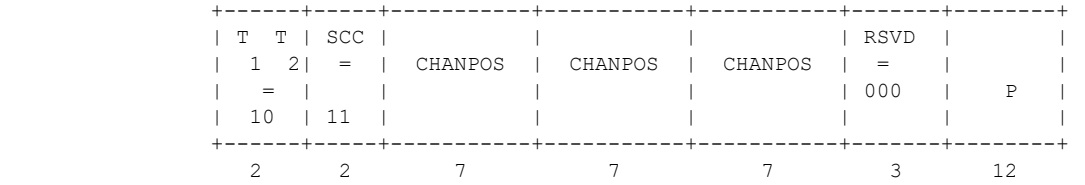
Слово 1 (сокращённое адресное слово)



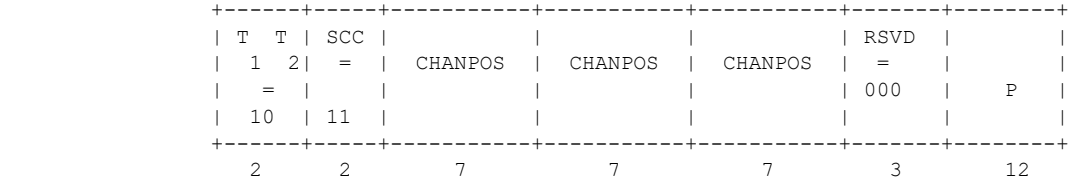
Слово 2 (расширенное адресное слово)



Слово 3 (первое слово направленного повтора)



Слово 4 (второе слово направленного повтора)



Интерпретация полей данных:

• **T1 T2** — поле типа. Если передаётся только слово 1, устанавливается в 00 в слове 1.
• **SCC** — цветовой код SAT (обсуждался ранее).
• **ORDER** — поле команды. Идентифицирует тип команды (см. таблицу ниже).
• **ORDQ** — поле квалификатора команды. Конкретизирует команду до определённого действия.
• **LOCAL** — поле локального управления. Специфично для каждой системы. Поле ORDER должно быть установлено на «локальное управление» для интерпретации этого поля.

• **VMAC** — поле кода ослабления голосового мобильного. Указывает уровень мощности мобильной станции, связанный с назначенным голосовым каналом.
• **CHAN** — поле номера канала. Указывает назначенный голосовой канал.
• **CHANPOS** — поле позиции канала. Указывает позицию управляющего канала относительно первого канала доступа (FIRSTCHA).
• **RSVD** — зарезервировано для будущего использования, все биты должны быть установлены как указано.
• **P** — поле чётности.

Кодированный цифровой цветовой код

Принятый DCC	7-битный DCC
00	0000000
01	0011111
10	1100011
11	1111100

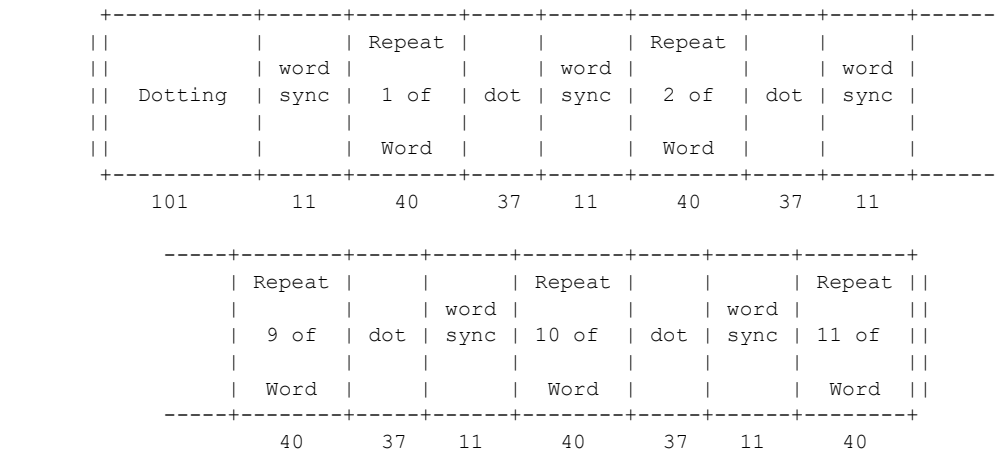
Коды команд и квалификаторов команд

Код команд.	Код квалификатора команды	Функция
00000	000	вызов (или исходящий)
00001	000	оповещение
00011	000	освобождение
00100	000	переадресация
00110	000	остановить оповещение
00111	000	аудит
01000	000	отправить адрес вызываемого
01001	000	перехват
01010	000	обслуживание
01011	000	изменить мощность до уровня 0
01011	001	изменить мощность до уровня 1
01011	010	изменить мощность до уровня 2
01011	011	изменить мощность до уровня 3
01011	100	изменить мощность до уровня 4
01011	101	изменить мощность до уровня 5
01011	110	изменить мощность до уровня 6
01011	111	изменить мощность до уровня 7
01100	000	направленный повтор — не последняя попытка
01100	001	направленный повтор — последняя попытка
01101	000	неавтономная регистрация — не раскрывать местоположение
01101	001	неавтономная регистрация — сообщить местоположение
01101	010	автономная регистрация — не раскрывать местоположение
01101	011	автономная регистрация — сообщить местоположение
11110	000	локальное управление
Все прочие коды зарезервированы		

Прямой голосовой канал (Forward Voice Channel)

Прямой голосовой канал (FVC) — широкополосный поток данных, передаваемый наземной станцией мобильной. Этот поток должен генерироваться со скоростью 10 кбит/с, ±0,1 бит/с. Формат

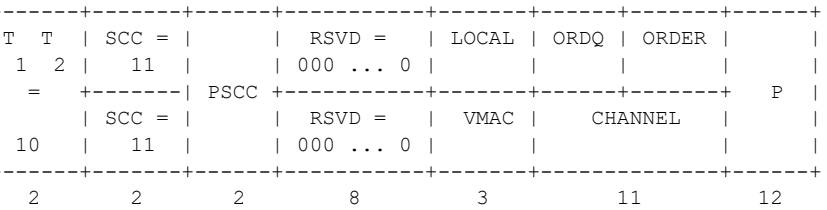
прямого голосового канала:



37-битная последовательность точек и 11-битная последовательность синхронизации слова передаются для синхронизации мобильных станций с входящими данными, за исключением первого повтора слова, где используется 101-битная последовательность точек. Каждое слово содержит 40 бит, включая биты чётности, и повторяется одиннадцать раз вместе с 37-битными точками и 11-битной синхронизацией; такой блок именуется «блоком слова». Блок слова формируется кодированием 28 информационных бит в (40, 28) BCH-код с расстоянием 5 — (40, 28; 5). Крайний левый бит обозначается как наиболее значимый. 28 наиболее значимых бит 40-битного поля являются информационными битами. Порождающий полином совпадает с используемым для прямого управляющего канала.

По прямому голосовому каналу передаётся только управляющее сообщение для мобильной станции, которое состоит из одного слова.

Управляющее сообщение для мобильной станции:

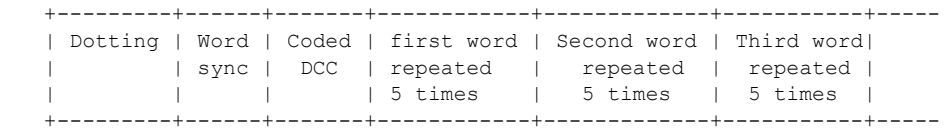


Интерпретация полей данных:

• **T1 T2** — поле типа. Устанавливается в «10».
• **SCC** — цветовой код SAT для нового канала (см. таблицу SCC).
• **PSCC** — текущий цветовой код SAT. Указывает цветовой код SAT, связанный с текущим каналом.
• **ORDER** — поле команды. Идентифицирует тип команды (см. таблицу команд).
• **ORDQ** — поле квалификатора команды. Конкретизирует команду до определённого действия (см. таблицу команд).
• **LOCAL** — поле локального управления. Специфично для каждой системы. Поле ORDER должно быть установлено на «локальное управление» (см. таблицу команд) для интерпретации данного поля.
• **VMAC** — поле кода ослабления голосового мобильного. Указывает уровень мощности мобильной станции, связанный с назначенным голосовым каналом.
• **RSVD** — зарезервировано для будущего использования; все биты должны быть установлены как указано.
• **P** — поле чётности.

Обратный управляющий канал (Reverse Control Channel)

Обратный управляющий канал (RECC) — широкополосный поток данных, передаваемый от мобильной станции к наземной. Этот поток работает со скоростью 10 кбит/с, ±1 бит/с. Формат потока данных RECC:



Dotting = 01010101...010101

Word sync = 11100010010

Все сообщения начинаются с преамбулы захвата RECC, которая состоит из 30-битной последовательности точек (1010...101), 11-битной последовательности синхронизации слова (11100010010) и кодированного цифрового цветового кода.

Каждое слово содержит 48 бит, включая биты чётности, и повторяется пять раз, после чего именуется «блоком слова». Слово формируется кодированием 36 информационных бит в (48, 36) BCH-код с расстоянием 5 — (48, 36; 5). Крайний левый бит обозначается как наиболее значимый. 36 наиболее значимых бит 48-битного поля являются информационными.

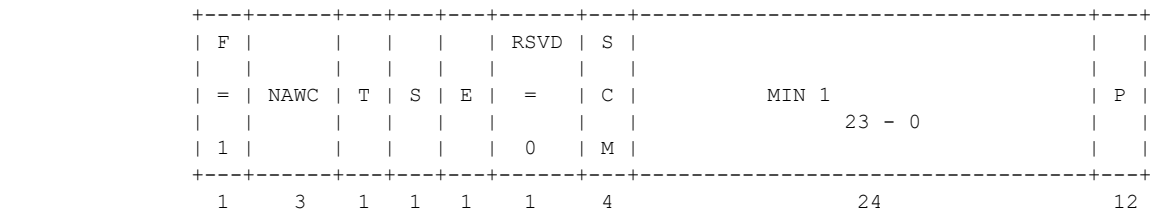
Порождающий полином кода совпадает с (40, 28; 5)-кодом, используемым на прямом канале.

Каждое сообщение обратного управляющего канала может состоять из одного из пяти слов. Типы сообщений, передаваемых по обратному управляющему каналу:

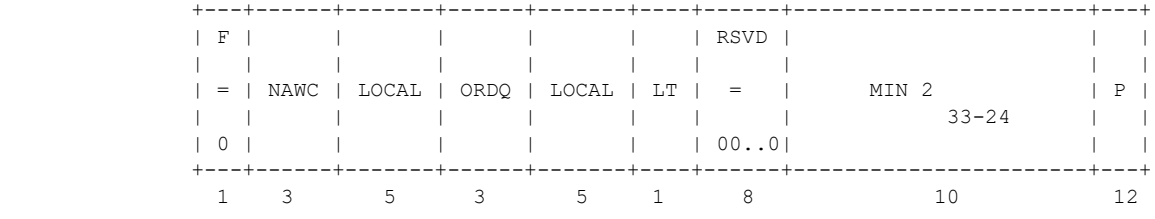
• Сообщение ответа на вызов
• Сообщение исходящего вызова
• Сообщение подтверждения команды
• Сообщение команды

Эти сообщения составляются из комбинаций следующих пяти слов:

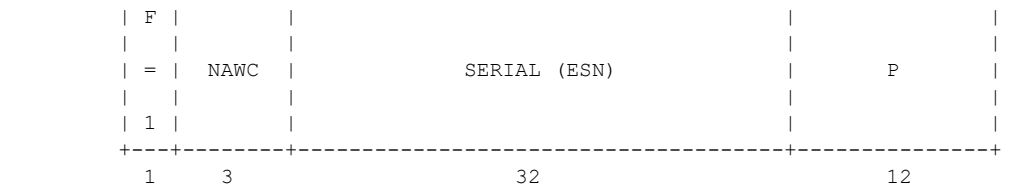
Слово A — сокращённое адресное слово



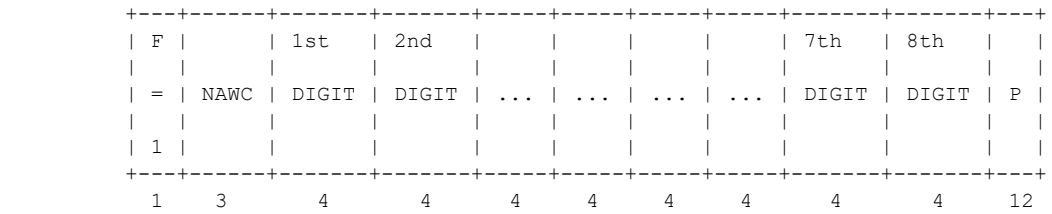
Слово B — расширенное адресное слово



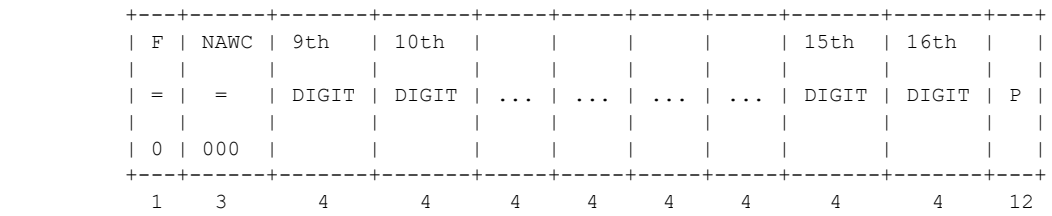
Слово C — слово электронного серийного номера



Слово D — первое слово адреса вызываемого



Слово E — второе слово адреса вызываемого



F					RSVD	S		
=	NAWC	T	S	E	=	C	MIN 1	P
							23 - 0	
1					0	M		

Интерпретация полей данных:

• **F** — поле признака первого слова. Устанавливается в «1» в первом слове и в «0» в последующих.
• **NAWC** — поле количества дополнительных слов.
• **T** — поле T. Устанавливается в «1» для обозначения исходящего вызова или команды; в «0» — для ответа на команду или на вызов.
• **S** — поле «отправить слово серийного номера». «1» — если слово серийного номера отправляется; «0» — если нет.
• **SCM** — поле метки класса станции.
• **ORDER** — поле команды. Идентифицирует тип команды.
• **ORDQ** — поле квалификатора команды. Конкретизирует подтверждение команды до определённого действия.
• **LOCAL** — поле локального управления. Специфично для каждой системы. Поле ORDER должно быть установлено на «локальное управление» для интерпретации данного поля.
• **LT** — поле кода последней попытки.
• **MIN1** — первая часть поля идентификационного номера мобильного.
• **MIN2** — вторая часть поля идентификационного номера мобильного.
• **SERIAL** — поле электронного серийного номера. Идентифицирует серийный номер мобильной станции.
• **DIGIT** — поле цифры (см. таблицу ниже).

• **RSVD** — зарезервировано для будущего использования; все биты должны быть установлены как указано.
• **P** — поле чётности.

Коды цифр адреса вызываемого

Цифра	Код	Цифра	Код
1	0001	7	0111
2	0010	8	1000
3	0011	9	1001
4	0100	0	1010
5	0101	*	1011
6	0110	#	1100
		Null	0000

ПРИМЕЧАНИЕ:
1. Цифра 0 кодируется как двоичное 10, а не двоичный ноль.
2. Код 0000 является нулевым кодом, означает отсутствие цифры.
3. Все прочие четырёхбитные последовательности зарезервированы и не должны передаваться.

Примеры кодирования адреса вызываемого в слова адреса:

Если введён номер 2#, слово выглядит следующим образом:

NOTE									P
	0010	1100	0000	0000	0000	0000	0000	0000	

Если введён номер 13792640, слово выглядит следующим образом:

NOTE									P
	0001	0011	0111	1001	0010	0110	0100	1010	

Как видно, числа кодируются в четыре бита и последовательно вставляются в поток. Обратите внимание: если номер длиннее 8 цифр, он разбивается на два разных слова.

Если введён номер 6178680300, слова выглядят следующим образом:

Слово D — первое слово адреса вызываемого

NOTE									P
	0110	0001	0111	1000	0110	1000	1010	1010	
4	4	4	4	4	4	4	4	4	12

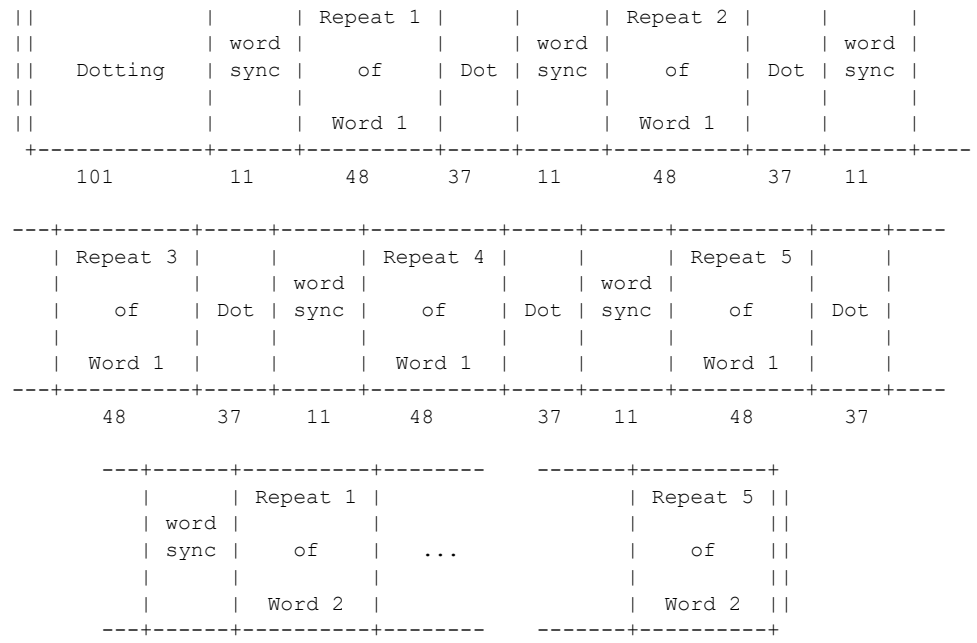
Слово E — второе слово адреса вызываемого

NOTE									P
	0010	1010	1010	0000	0000	0000	0000	0000	
4	4	4	4	4	4	4	4	4	12

NOTE = четыре бита, зависящих от типа сообщения

Обратный голосовой канал (Reverse Voice Channel)

Обратный голосовой канал (RVC) — широкополосный поток данных, передаваемый от мобильной станции к наземной. Этот поток должен генерироваться со скоростью 10 кбит/с, ±1 бит/с. Формат представлен ниже.



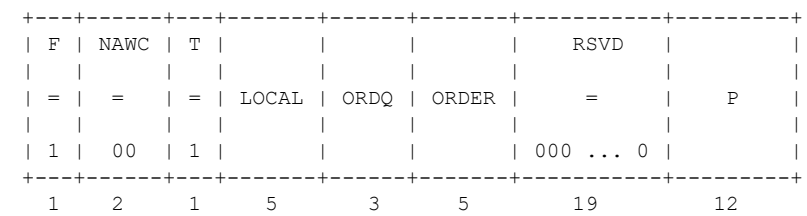
37-битная последовательность точек и 11-битная последовательность синхронизации слова передаются для синхронизации наземных станций с входящими данными, за исключением первого повтора слова 1, где используется 101-битная последовательность точек. Каждое слово содержит 48 бит, включая биты чётности, и повторяется пять раз вместе с 37-битными точками и 11-битной синхронизацией; такой блок именуется «блоком слова». В многословном сообщении второй блок формируется так же, как и первый, включая 37-битные точки и 11-битную синхронизацию. Слово формируется кодированием 36 информационных бит в (48, 36) BCH-код с расстоянием 5 — (48, 36; 5). Крайний левый бит (самый ранний по времени) обозначается как наиболее значимый. 36 наиболее значимых бит 48-битного поля являются информационными. Порождающий полином кода совпадает с (40, 28; 5)-кодом, используемым на прямом управляющем канале.

Каждое сообщение RVC может состоять из одного или двух слов. Типы сообщений, передаваемых по обратному голосовому каналу:

• Сообщение подтверждения команды
• Сообщение адреса вызываемого

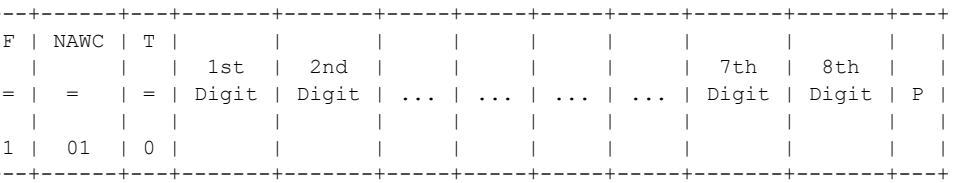
Форматы сообщений:

Сообщение подтверждения команды:



Сообщение адреса вызываемого

Слово 1 — первое слово адреса вызываемого



```
  1    2     1     4       4      4     4     4     4      4       4     12
```

Слово 2 — второе слово адреса вызываемого

```
  +---+------+---+-------+-------+-----+-----+-----+-----+-------+-------+---+
  | F | NAWC | T |       |       |     |     |     |     |       |       |   |
  |   |      |   |  9th  |  10th |     |     |     |     |  15th |  16th |   |
  | = |  =   | = | Digit | Digit | ... | ... | ... |  .. | Digit | Digit | P |
  |   |      |   |       |       |     |     |     |     |       |       |   |
  | 0 |  00  | 0D|       |       |     |     |     |     |       |       |   |
  +---+------+---+-------+-------+-----+-----+-----+-----+-------+-------+---+
    1    2     1     4       4      4     4     4     4      4       4     12
```

Описания полей аналогичны описаниям для обратного управляющего канала, приведённым выше.

Служебное сообщение (Overhead Message)

Трёхбитное поле OHD используется для идентификации типов служебных сообщений. Коды типов служебных сообщений перечислены в таблице ниже. Они разделены на следующие функциональные классы:

• Служебное сообщение системных параметров
• Служебное сообщение глобальных действий
• Сообщение идентификации регистрации
• Сообщение управляющего заполнителя

Служебные сообщения передаются в группе, называемой «поездом служебных сообщений» (overhead message train). Первым в поезде должно быть служебное сообщение системных параметров. Нужные сообщения глобальных действий и/или сообщение идентификации регистрации должны добавляться в конец служебного сообщения системных параметров. Общее число слов в поезде служебных сообщений на единицу больше значения поля NAWC, содержащегося в первом слове служебного сообщения системных параметров. Последнее слово поезда должно быть установлено в «0». Для целей подсчёта NAWC вставленные сообщения управляющего заполнителя не учитываются как часть поезда служебных сообщений.

Служебное сообщение системных параметров должно передаваться каждые 0,8 ±0,3 секунды по каждому из следующих управляющих каналов:

• Совмещённый прямой канал вызова и доступа.
• Отдельный прямой управляющий канал вызова.
• Отдельный прямой управляющий канал доступа, когда сообщение управляющего заполнителя передаётся с битом WFOM, установленным в «1».

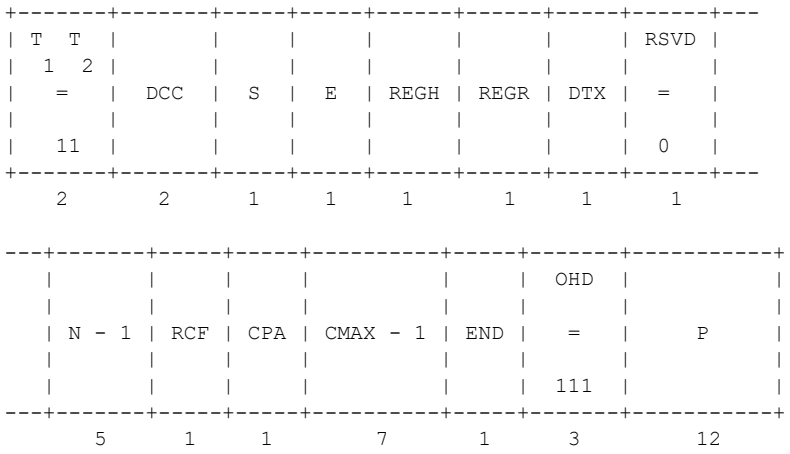
Сообщения глобальных действий и сообщение идентификации регистрации передаются по мере необходимости.

Служебное сообщение системных параметров состоит из двух слов.

Слово 1

```
  +-------+-----+----------+------+------+-----+------------+
  | T  T  |     |          | RSVD |      | OHD |            |
  |  1  2 |     |          |      |      |     |            |
  |   =   | DCC |   SID1   |  =   | NAWC |  =  |     P      |
  |       |     |          |      |      |     |            |
  |  11   |     |          | 000  |      | 110 |            |
  +-------+-----+----------+------+------+-----+------------+
      2      2       14        3      4     3        12
```

Слово 2



Типы служебных сообщений

Код	Тип
000	Идентификатор регистрации
001	Управляющий заполнитель
010	зарезервировано
011	зарезервировано
100	Глобальное действие
101	зарезервировано
110	Слово 1 сообщения системных параметров
111	Слово 2 сообщения системных параметров

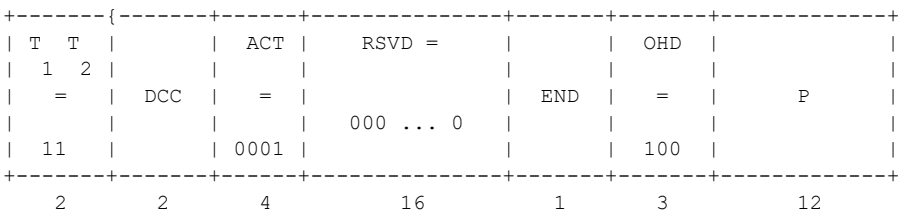
Интерпретация полей данных:

• **T1 T2** — поле типа. Установлено в «11», указывая на служебное слово.
• **OHD** — поле типа служебного сообщения. Поле OHD слова 1 установлено в «110» — первое слово служебного сообщения системных параметров. Поле OHD слова 2 установлено в «111» — второе слово.
• **DCC** — поле цифрового цветового кода.
• **SID1** — первая часть поля идентификатора системы.
• **NAWC** — поле количества дополнительных слов. В слове 1 устанавливается в значение на единицу меньше общего числа слов в поезде служебных сообщений.
• **S** — поле серийного номера.
• **E** — поле расширенного адреса.
• **REGH** — поле регистрации для домашних станций.
• **REGR** — поле регистрации для роуминговых станций.
• **DTX** — поле прерывистой передачи.
• **N-1** — N — количество каналов вызова в системе.
• **RCF** — поле чтения управляющего заполнителя.
• **CPA** — поле совмещённого вызова и доступа.
• **CMAX-1** — CMAX — количество каналов доступа в системе.
• **END** — поле признака завершения. «1» — последнее слово; «0» — не последнее.
• **RSVD** — зарезервировано для будущего использования; все биты должны быть установлены как указано.
• **P** — поле чётности.

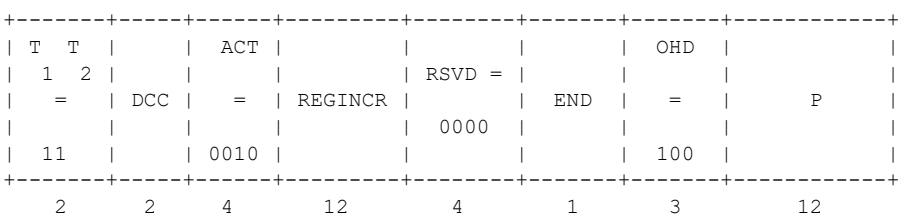
Каждое служебное сообщение глобальных действий состоит из одного слова. К служебному сообщению системных параметров может быть добавлено любое количество сообщений глобальных действий.

Форматы команд глобальных действий:

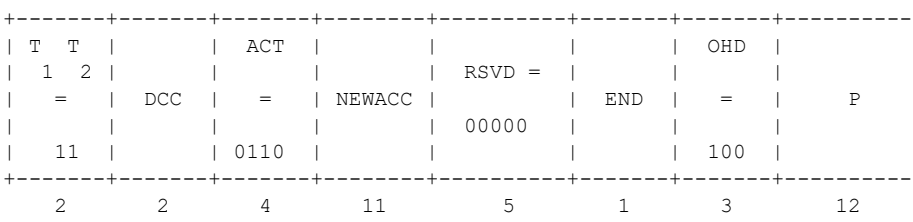
Сообщение глобального действия «Повторное сканирование» (Rescan)



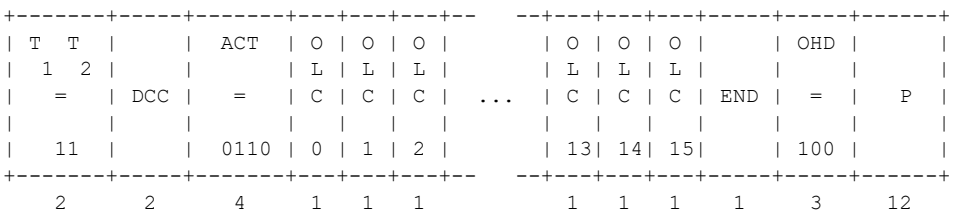
Сообщение глобального действия «Шаг регистрации» (Registration Increment)



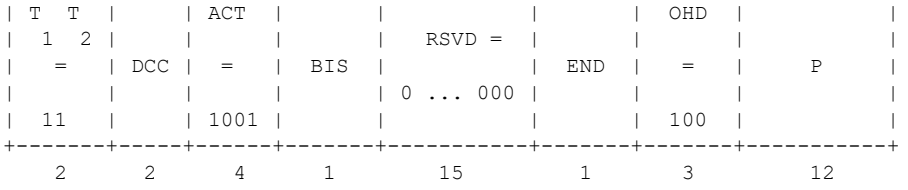
Сообщение глобального действия «Новый набор каналов доступа»



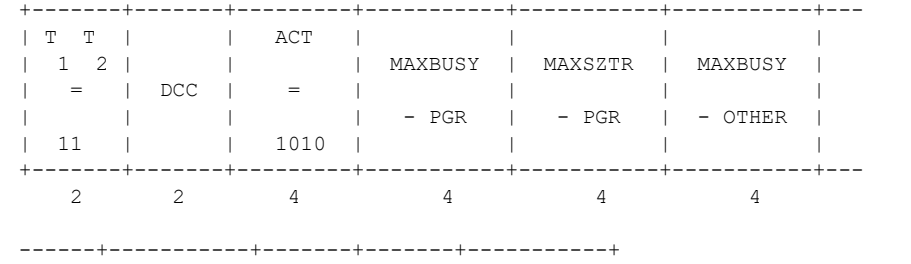
Сообщение глобального действия «Управление перегрузкой»



Сообщение глобального действия «Параметры типа доступа»



Сообщение глобального действия «Параметры попыток доступа»



```
      |  MAXSZTR  |       |       |           |
      |           |  END  |   =   |     P     |
      |  - OTHER  |       |       |           |
      |           |       |  100  |           |
------+-----------+-------+-------+-----------+
            4         1       3         12
```

Сообщение локального управления 1

```
+-------+-------+-------+-----------------+-------+-------+----------+
| T  T  |       |  ACT  |                 |       |  OHD  |          |
|  1  2 |       |       |                 |       |       |          |
|   =   |  DCC  |   =   |  LOCAL CONTROL  |  END  |   =   |     P    |
|       |       |       |                 |       |       |          |
|   11  |       |  1110 |                 |       |  100  |          |
+-------+-------+-------+-----------------+-------+-------+----------+
    2       2       4            16           1       3        12
```

Сообщение локального управления 2

```
+-------+-------+-------+-----------------+-------+-------+----------+
| T  T  |       |  ACT  |                 |       |  OHD  |          |
|  1  2 |       |       |                 |       |       |          |
|   =   |  DCC  |   =   |  LOCAL CONTROL  |  END  |   =   |     P    |
|       |       |       |                 |       |       |          |
|   11  |       |  1111 |                 |       |  100  |          |
+-------+-------+-------+-----------------+-------+-------+----------+
    2       2       4            16           1       3        12
```

T T		ACT	RSVD =		OHD	
1 2						
=	DCC	=		END	=	P
			000 ... 0			
11		0001			100	

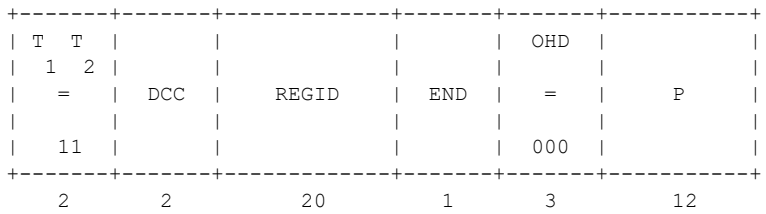
T T		ACT	RSVD =		OHD	
1 2						
=	DCC	=		END	=	P
			000 ... 0			
11		0001			100	

Интерпретация полей данных:

• **T1 T2** — поле типа. Установлено в «11», указывая на служебное слово.
• **ACT** — поле глобального действия (см. таблицу ниже).
• **BIS** — поле статуса «занято-свободно».
• **DCC** — цифровой цветовой код.
• **OHD** — поле типа служебного сообщения. Установлено в «100» для служебного сообщения глобальных действий.
• **REGINCR** — поле шага регистрации.

• **NEWACC** — поле начальной точки нового канала доступа.
• **MAXBUSY - PGR** — максимальное число событий занятости (ответ на вызов).
• **MAXBUSY - OTHER** — максимальное число событий занятости (прочие виды доступа).
• **MAXSZTR - PRG** — максимальное число попыток захвата (ответ на вызов).
• **MAXSZTR - OTHER** — максимальное число попыток захвата (прочие виды доступа).
• **OLCN** — поле класса перегрузки (N = от 0 до 15).
• **END** — поле признака завершения. «1» — последнее слово поезда служебных сообщений; «0» — не последнее.
• **RSVD** — зарезервировано для будущего использования; все биты должны быть установлены как указано.
• **LOCAL CONTROL** — может принимать любой битовый образец.
• **P** — поле чётности.

Сообщение идентификации регистрации состоит из одного слова. При передаче оно должно добавляться к служебному сообщению системных параметров в дополнение к любым сообщениям глобальных действий.

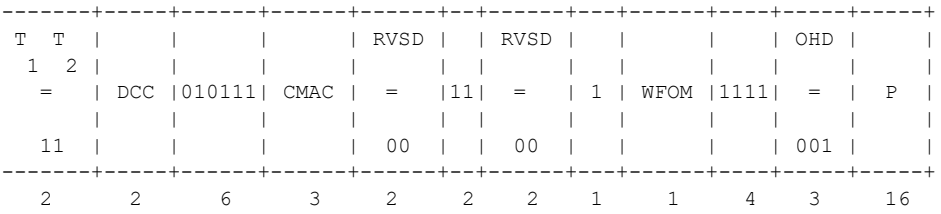


Интерпретация полей данных:

• **T1 T2** — поле типа. Установлено в «11», указывая на служебное слово.
• **DCC** — поле цифрового цветового кода.
• **OHD** — поле типа служебного сообщения. Установлено в «000» — сообщение идентификации регистрации.
• **REGID** — поле идентификатора регистрации.
• **END** — поле признака завершения. «1» — последнее слово; «0» — нет.
• **P** — поле чётности.

Сообщение управляющего заполнителя состоит из одного слова. Оно передаётся всякий раз, когда нет другого сообщения для отправки по прямому управляющему каналу. Оно может вставляться между сообщениями, а также между блоками слов многословного сообщения. Сообщение управляющего заполнителя выбрано таким образом, что при его передаче 11-битная последовательность синхронизации слова не появляется в потоке сообщений — независимо от состояния бита занято-свободно.

Сообщение управляющего заполнителя также используется для задания кода ослабления мобильного на управляющем канале (CMAC) для использования мобильными станциями, обращающимися к системе через обратный управляющий канал, и бита ожидания служебного сообщения (WFOM), указывающего, обязаны ли мобильные станции читать поезд служебных сообщений перед обращением к системе.



Интерпретация полей данных:

• **T1 T2** — поле типа. Установлено в «11», указывая на служебное слово.
• **DCC** — поле цифрового цветового кода.
• **CMAC** — поле ослабления мобильного на управляющем канале. Указывает уровень мощности мобильной станции, связанный с обратным управляющим каналом.
• **RVSD** — зарезервировано для будущего использования; все биты должны быть установлены как указано.
• **WFOM** — поле ожидания служебного сообщения.
• **OHD** — поле типа служебного сообщения. Установлено в «001» — слово управляющего заполнителя.
• **P** — поле чётности.

Ограничения на данные

11-битная последовательность (11100010010) короче, чем длина слова, и поэтому может быть встроена в слово. Как правило, встроенная синхронизация слова не вызывает проблем, поскольку следующее переданное слово не будет содержать встроенной последовательности синхронизации. Тем не менее существуют три случая, в которых последовательность синхронизации слова может периодически появляться в потоке FOCC:

• служебное сообщение;
• сообщение управляющего заполнителя;
• управляющие сообщения для мобильных станций с вызовами мобильных с определёнными кодами АТС.

Эти три случая обрабатываются следующим образом:

1. Ограничением частоты передачи служебных сообщений примерно до одного раза в секунду.
2. Конструированием сообщения управляющего заполнителя так, чтобы исключить последовательность синхронизации слова с учётом различных битов занято-свободно.
3. Ограничением использования определённых кодов АТС.

Если рассмотреть управляющее сообщение мобильной станции, в котором MIN1 разделён на NXX-X-XXX, как описано ранее (где NXX — код АТС, N — цифра от 2 до 9, X — цифра от 0 до 9), таблица команд и квалификаторов команд может использоваться для определения того, когда будет передано слово синхронизации слова. Если ряд мобильных станций вызывается подряд с одним и тем же кодом АТС, мобильные, пытающиеся синхронизироваться с потоком данных, могут оказаться не в состоянии сделать это из-за наличия ложной последовательности синхронизации слова. Поэтому комбинации кодов АТС и групп абонентских номеров, приведённые в следующей таблице, не должны использоваться для мобильных станций.

ЗАПРЕЩЁННЫЕ КОДЫ ЦЕНТРАЛЬНЫХ ОФИСОВ (АТС)

T 1	T 2	DCC	NXX	X	XXX	Центральный офис (АТС)	Тысячный разряд
01		11	000100(1)0000	...	...	175	0 to 9
01		11	000100(1)0001	...	...	176	0 to 9
01		11	000100(1)0010	...	...	177	0 to 9
01		11	000100(1)0011	...	...	178	0 to 9
01		11	000100(1)0100	...	...	179	0 to 9
01		11	000100(1)0101	...	...	170	0 to 9
01		11	000100(1)0110	...	...	181	0 to 9
01		11	000100(1)0111	...	...	182	0 to 9
0Z		11	100010(0)1000	...	...	663	0 to 9
0Z		11	100010(0)1001	...	...	664	0 to 9

0Z	11	100010(0)1010	...	...	665	0 to 9
0Z	11	100010(0)1011	...	...	666	0 to 9
0Z	Z1	110001(0)0100	...	...	899	0 to 9
0Z	Z1	110001(0)0101	...	...	800	0 to 9
0Z	ZZ	111000(1)0010	...	...	909	0 to 9
00	ZZ	011100(0)1001	0ZZZ	...	568	1 to 7
00	ZZ	111100(0)1001	0ZZZ	...	070	1 to 7
00	ZZ	001110(0)0100	10ZZ	...	339	8,9,0
00	ZZ	011110(0)0100	10ZZ	...	595	8,9,0
00	ZZ	101110(0)0100	10ZZ	...	851	8,9,0
00	ZZ	111110(0)0100	10ZZ	...	007	8,9,0
0Z	ZZ	000011(1)0100	0010	...	150	2
0Z	ZZ	000111(1)0001	0010	...	224	2
0Z	ZZ	001011(1)0001	0010	...	288	2
0Z	ZZ	001111(1)0001	0010	...	352	2
0Z	ZZ	010011(1)0001	0010	...	416	2
0Z	ZZ	010111(1)0001	0010	...	470	2
0Z	ZZ	011011(1)0001	0010	...	544	2
0Z	ZZ	011111(1)0001	0010	...	508	2
0Z	ZZ	100011(1)0001	0010	...	672	2
0Z	ZZ	100111(1)0001	0010	...	736	2
0Z	ZZ	101011(1)0001	0010	...	790	2
0Z	ZZ	101111(1)0001	0010	...	864	2
0Z	ZZ	110011(1)0001	0010	...	928	2
0Z	ZZ	110111(1)0001	0010	...	992	2
0Z	ZZ	111011(1)0001	0010	...	056	2
0Z	ZZ	111111(1)0001	0010	...	...	2

1. В каждом случае Z обозначает бит, который может быть равен 1 или 0.
2. Некоторые коды в настоящее время не используются в США в качестве кодов ATC. Они включены для полноты.
3. Бит в скобках — бит занято-свободно.

Итак, вот вам сигнализация в двух словах. Обратите внимание: у меня нет самых актуальных данных о сигнализации. По существу, здесь был представлен скелет — голые кости без всех дополнений. Некоторые из них специфичны для конкретных систем. По мере получения обновлений я обязательно поделюсь ими с вами. Мне был бы интересен любой отклик, поэтому, если вам есть что сказать, пишите на:

oblivion@atdt.org

В прошлой статье я упомянул, что к ней будет прилагаться список кодов SID. Ну что же — я забыл убрать эту строку, но если вам нужна копия, просто напишите мне по указанному выше адресу, и вы её получите.

В следующей статье я подробно рассмотрю аппаратную составляющую мобильного телефона, используемые наборы микросхем и принципы их работы. Также я опубликую любые обновления к предыдущим материалам, которые обнаружу, а также информацию о переходной системе NAMPS, которая должна обеспечить мост между существующей сотовой сетью AMPS и полностью цифровой сетью, совместимой с ISDN.

Высокое искусство телефонии

```
=/=/=/=/=/=/=/=^=\=\=\=\=\=\=\=
=                              =
=  The Fine Art of Telephony   =
=                              =
=       by Crimson Flash       =
=                              =
=\=\=\=\=\=\=\=!=/ =/=/=/=/=/=/=
```

Автор: Crimson Flash

Белл! Белл! Белл! Твоё царствование тирании под угрозой, твои тайны будут преданы огласке. Хакеры пришли заявить о своих правах и пробить бреши в твоём монопольном контроле. Девяностые начались с нападения на нас, но завершатся нашей победой — разоблачением тайного правительства и коррупции, скрытой за твоими стенами и экранами. Противься нам со всей своей мощью, со всей своей ложью, со всеми своими бухгалтерами и липовыми «профессионалами» безопасности. Одного ты, может, и остановишь — но многих тебе не остановить никогда.

A. Введение

Белл. Белл Белл Белл! Что же такого в Bell? Я сам не знаю, чем они меня так притягивают, но этот интерес не утихает и не ослабевает. Возможно, всё дело в том, что они такие закрытые. Возможно, потому что им удаётся ежедневно обирать миллионы людей — и делают они это с такой поразительной лёгкостью. Или, быть может, просто потому что они не хотят, чтобы кто-нибудь знал, что они делают.

В моём районе, здесь в Техасе (512), здания Центральных Офисов обнесены высокими кирпичными стенами, на каждой двери — камера, везде яркое освещение, и на каждой бумаге крупными буквами написано: «PROPRIETARY INFORMATION — NOT FOR USE OR DISCLOSURE OUTSIDE OF SOUTHWESTERN BELL» («Конфиденциальная информация — не для использования или раскрытия за пределами Southwestern Bell»). Это сообщение встречается повсюду — кроме, пожалуй, телефонных книг! Почему?

Этот файл посвящён RCMAC и FACS/MARCH. Информация здесь в основном по памяти. Если считаете, что что-то не так — добудьте информацию сами! Важно помнить: ничто не высечено в камне. Разные BOC (Bell Operating Companies, дочерние компании Bell) используют разные системы и по-разному делают одно и то же. Например, в одних районах RCMAC называется CIC, MLAC может отсутствовать вовсе, и так далее. Так что у Bell ничто никогда не бывает полностью верным — но почему её системы должны отличаться от её политики и обещаний? Есть стандарт Bellcore, а есть то, как это реально делается в вашем местном BOC.

B. Основы коммутации

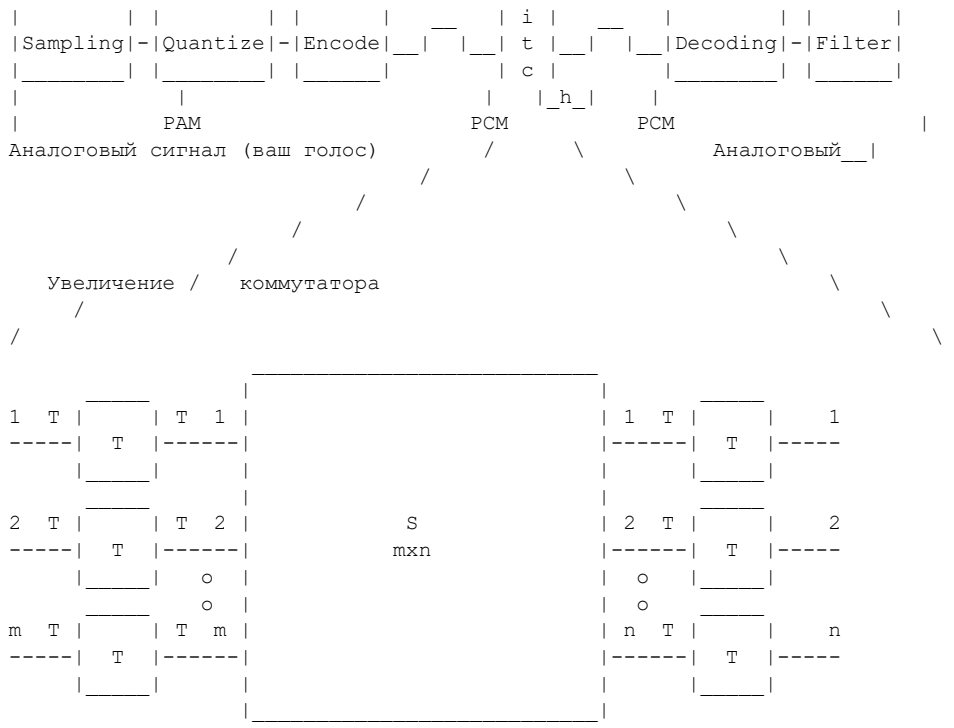
Коммутационная система (коммутатор) позволяет устанавливать соединение между двумя (или более) телефонными линиями или двумя магистральными каналами. Базовый канал T1 — это 24 линии на 4-жильной витой паре 22-го калибра. Коммутатор не только устанавливает соединение, но и управляет им: куда вы звоните и когда вам звонят. Короче говоря, он управляет всем, что касается вашего телефона! От огромного AT&T 5ESS, обслуживающего 150 000+ линий, до маленького 24-линейного PABX (Private Automatic Branch Exchange — мини-АТС), — все они контролируют вашу телефонную связь.

В чём значимость телефонных коммутаторов? Телефония — это крупнейший вид связи практически для каждого человека в мире! Попробуйте пожить без телефонной линии в доме. У меня четыре телефонных линии, и порой этого всё равно недостаточно.

Современные коммутаторы — цифровые. Это значит, что когда вы говорите по телефону, ваш голос преобразуется в единицы и нули (включено или выключено, истина или ложь). Процесс состоит из нескольких шагов:

```
[0] Вы звоните кому-то.
[1] Выборка (Sampling) — аналоговый сигнал (ваш голос) считывается
    в определённых точках. Результат называется сигналом с импульсно-
    амплитудной модуляцией (PAM).
[2] Квантование (Quantize) — PAM-сигнал измеряется по высоте волны
    (амплитуде), значениям присваиваются числа.
[3] Кодирование (Encoding) — квантованный сигнал (с числами,
    представляющими высоту амплитуды) преобразуется в 8-битное
    двоичное число. Выходное 8-битное «слово» может быть либо «1»
    (импульс), либо «0» (нет импульса).
[4] Кодирование (Encoding) — формируется сигнал с импульсно-кодовой
    модуляцией (PCM). PCM просто означает, что сигнал модулирует
    импульсы (цифровой). С этой точки сигнал переключается туда,
    куда нужно.
[5] PCM-сигнал доставлен по назначению. Теперь сигнал преобразуется
    обратно в аналоговый.
[6] Декодирование (Decoding) — 8-битный PCM-сигнал поступает в
    декодер для получения числа, измерявшего амплитуду волны.
[7] Фильтрация (Filtering) — PAM-сигнал (полученный после
    декодирования) воспроизводит аналоговый сигнал в исходном виде.


                                  ___
[1]          [2]       [3]     [4]  | S |  [5]       [6]      [7]
 ________   _________  ______       | w |         ________   ______
```



Основной принцип построения большинства современных коммутаторов — топология «Время–Пространство–Время» (TST). В схеме TST в показанном расположении переключатели временных интервалов (time slot interchangers) обменивают информацию между внешними каналами и внутренними (пространственная матрица) каналами.

Это лишь краткое введение, дающее общее представление о коммутаторах без углубления в математику и технические детали. Для более глубокого понимания рекомендую книгу «Fundamentals of Digital Switching» Джона К. Макдональда. Книга написана доступно и описывает идеи, которые здесь нет возможности рассмотреть.

C. RCMAC

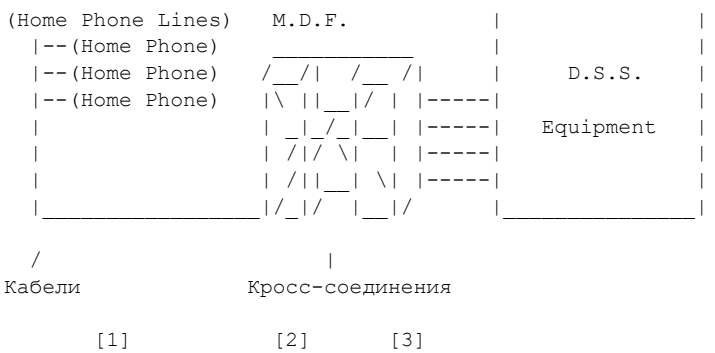
Назначение RCMAC (Recent Change Memory Administration Center — Центр администрирования памяти изменений) — вносить изменения в программное обеспечение различных электронных коммутационных систем (ESS). ESS использует программное управление с хранимой программой (SPC) для предоставления телефонных услуг. Поскольку абоненты и их услуги часто меняются, ESS использует область памяти под названием Recent Change («Последние изменения»). Эта область памяти задействуется на резервной основе до тех пор, пока информация не будет обновлена в полупостоянной области памяти ESS. Именно в этой временной области вводятся и хранятся изменения (или сообщения об изменениях) для последующего обновления в полупостоянную память (Recent Change Memory).

Следующие коммутационные системы (коммутаторы) поддерживают Recent Change:

- 1/1AESS
- 2/2BESS
- 3ESS
- 5ESS
- Remote Switching System (RSS)
- #5ETS
- DMS100/200/250/300

Вот типичная схема подключения. По мере изучения диаграммы ниже вы увидите:

```
[1] Телефонный абонент подключён к Центральному Офису кабелями.
[2] В Центральном Офисе каждый абонент подключён к Главному
    распределительному фрейму (MDF).
[3] Кабельная пара теперь подключена к Офисному Оборудованию (OE)
    в другом месте на MDF.
```



1. Офисное оборудование

Офисное Оборудование (OE) идентифицируется уникальным планом нумерации. Номера оборудования определяют его расположение в системе. Номера также варьируются в зависимости от типа оборудования.

OE также может обозначаться как LEN (Line Equipment Number — Номер линейного оборудования). В случае RSS (Remote Switching System) используется термин REN (Remote Equipment Number — Номер удалённого оборудования).

Каждому телефонному номеру назначается конкретное место оборудования, где он получает тональный сигнал.

Примеры различных типов офисного оборудования:

```
1/1AESS
~~~~~~~
OE 0 0 4  - 1 0 1 - 3 1 2
   | |/     | | |   | |/
   | |      | | |   | |
   | |      | | |   | Level
   | |      | | |   Switch
   | |      | | Concentrator
   | |      | Bay
   | |  Line Switch Frame
   | Line Link
   Control Group
```

```
#2ESS
~~~~~
OE 0 1 1 - 2 1 4 0
   | |/    | | |/
   | |     | | |
   | |     | | Switch and Level
   | |     | Concentrator
   | |     Concentrator Group
   | Link Trunk Network
   Control Group
```

```
#3ESS
~~~~~
OE 0 0 1 - 2 1 4 0
   | |/    | | | |
   | |     | | | Level
   | |     | | Switch
   | |     | Switch Group
   | |     Concentrator
   | Concentrator Group
   Control Group
```

```
Прочие
~~~~~~
 1XB        =   XXXX-XXX-XX
 1XB        =   XXXX-XXXX-XX
 5XB        =   XXX-XX-XX
 SXS        =   XXXX-XXX
 DMS-10     =   XXX-X-XX-X
 5ESS       =   XXXX-XXX-XX
 5ESS       =   XXXX-XX-XX
 RSS        =   XXXX-X-XXXX
 DMS-1/200  =   XXX-X-XX-XX
```

2. Как всё это связано с RCMAC

RCMAC (Recent Change Memory Administration Center) отвечает за обновление любой активности Сервисных Заказов. Это действие изменяет клиентскую линию или услугу в памяти Recent Change коммутаторов с программным управлением (SPC).

3. Функции RCMAC

Три основные функции, выполняемые в RCMAC:

• a. Координация документации источников изменений
• b. Обработка запросов на изменения
• c. Административные обязанности и интерфейсные группы

Подробнее:

Координация документации источников изменений

Первая функция — координация исходных документов. Основным источником изменений (RC) являются Сервисные Заказы. Сервисные Заказы — это изменения в услугах абонента. RCMAC, помимо ввода сервисного заказа в коммутаторы, отвечает за другие виды деятельности:

• Симулированные группы объектов (SFG)
• Индексы маршрутов
• Регистры трафика (TR)
• Использование абонентских линий (SLU)
• Назначение наблюдения за обслуживанием (SOB)
• Обновления RPM MARCH (MIZAR)

Терминальные коммуникации с коммутаторами и/или MARCH (MIZAR) обычно используют AT&T Datakit. RCMAC также отвечает за «ГОРЯЧИЕ» запросы от Центра Установки (IC) и другие передачи от IC.

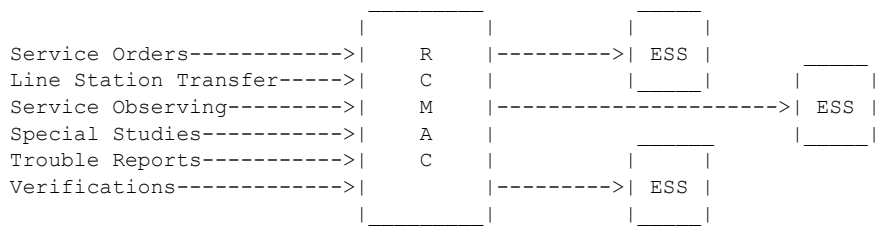
Обработка запросов на изменения

Вторая функция RCMAC — обработка сообщений RC. Это включает ввод и редактирование сообщений RC в коммутаторах. Когда RCMAC вводит сообщения, они вносят изменения в услугу клиента. Обслуживание клиентов зависит от своевременной и точной обработки исходных документов RC (Сервисных Заказов).

Дата исполнения (иногда называемая «Frame Due Date») и временной интервал, присвоенный заказу, определяют момент выпуска RC-ввода в ESS. Дата исполнения важна, поскольку это дата, к которой Сервисный Заказ должен быть выполнен (пройти систему FACS, завершить монтажные работы, и RC-сообщение должно быть введено в коммутатор).

Запросы на изменения (Recent Change Requests)

RCMAC получает документацию для изменений во временных областях памяти различных типов оборудования ESS. Эти изменения могут поступать в разных формах и из разных источников.



Некоторые запросы на Recent Change — это Сервисные Заказы, Переводы линейного оборудования (LET), Запросы на наблюдение за обслуживанием (SOB), Специальные

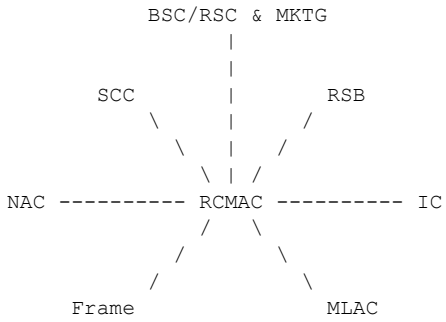
исследования (SLU), Отчёты об ошибках и Верификации (следуйте местным процедурам). Короче говоря, всё это — получение данной информации и внесение правильных изменений в коммутаторы SPC.

Административные обязанности и интерфейсные группы

• Контроль ошибок.
• Мониторинг активности.
• Подготовка административных отчётов.
• Координация операций RCMAC и взаимодействие с другими отделами.
• Восстановление области RC коммутаторов в случае повреждения памяти RC из-за сбоя оборудования.

Операционный интерфейс

RCMAC должен координировать деятельность со многими рабочими группами для обеспечения точного и быстрого RC для ESS.



Краткое описание каждой группы, взаимодействующей с RCMAC:

SCC (Switching Control Center — Центр управления коммутацией)

• Техническая помощь RCMAC.
• Обеспечение аварийного покрытия (в нерабочее время) для RCMAC. Включает проблемы, влияющие на обслуживание. Также координирует обновления программ ESS с RCMAC.

NAC (Network Administration Center — Центр администрирования сети) предоставляет RCMAC:

• Коды класса линии (LCC), например 1FR (1-party Flat Rate — Однопартийный фиксированный тариф).
• Список номеров, которые должны быть изменены (в памяти ESS) с одного индекса маршрута перехвата на другой, перед переназначением.
• Назначения трансляции; Пример: Simulated Facilities Group (SFG).
• Назначение Area Transfer/Dial for Dial.
• Назначение наблюдения за обслуживанием.
• Назначение исследования Subscriber Line Usages (SLU).
• Назначение исследования Customer Line Overflow.
• Обновления RPM для изменений DMS 100 в таблицах COSMOS USOC/NXX/Ltg.

Frame (Frame Jeopardy Reports — Отчёты о критическом состоянии монтажа) Центрального Офиса (FCC) взаимодействует с RCMAC по вопросам переводов линейного оборудования.

• Проблемы, возникающие у монтажной группы при выполнении Сервисных Заказов, могут быть скоординированы с MLAC (Loop Assignment Center), или при необходимости напрямую переданы в RCMAC (например, нет тонального сигнала на новом подключении).

Business/Residence Service Center (BSC/RSC) и Marketing (MKTG)

• BSC/RSC и MKTG определяют, какой вид обслуживания хочет клиент, формируют Сервисные Заказы и координируют с RCMAC специальные услуги для клиентов.

Repair Service Bureau (RSB) или Single Point of Contact (SPOC)

• Отчёты о неисправностях клиентов могут требовать RC-ввода; RCMAC тесно сотрудничает с RSB или SPOC для устранения таких неисправностей.
• RCMAC отвечает за анализ, расследование и устранение неисправностей клиентов, вызванных RC-вводом.

Installation Center (IC) и/или Maintenance Center (MC)

• Группа IC/MC отвечает за административную функцию, связанную с завершением и контролем нагрузки Сервисных Заказов. Это охватывает все заказы, требующие или не требующие полевых работ.
• Эта группа обеспечивает выполнение всех сервисных заказов в надлежащие сроки.

Mechanized Loop Assignment Center (MLAC) или LAC

• Назначает Сервисные Заказы для RCMAC.
• Назначает абонентские петли (эта группа есть не во всех BOC).

D. Среда FACS

Для лучшего понимания RCMAC, потока исходных документов и типичного BOC в целом, FACS (Facility Administration Control System — Система управления администрированием объектов) является важной её частью.

Системы в среде FACS

PREMIS — PREMises Information System (Система информации об объектах)
Эта система разделена на три части: основная база данных PREMIS, PREMLAC (Loop Assignment — Назначение петель) и PREMLAS (Loop Assignment Special circuit — Назначение специальных цепей петель). Содержит инвентарь клиентов и адресов, присваивает номера.

SOAC — Service Order Analysis and Control (Анализ и контроль сервисных заказов)
Эта система получает Сервисные Заказы от SORD, интерпретирует и определяет требования к объектам. Система запрашивает и получает назначения от LFACS и COSMOS, пересылает заказы в MARCH, пересылает назначения в SORD, а также ведёт историю Сервисных Заказов и управляет изменениями.

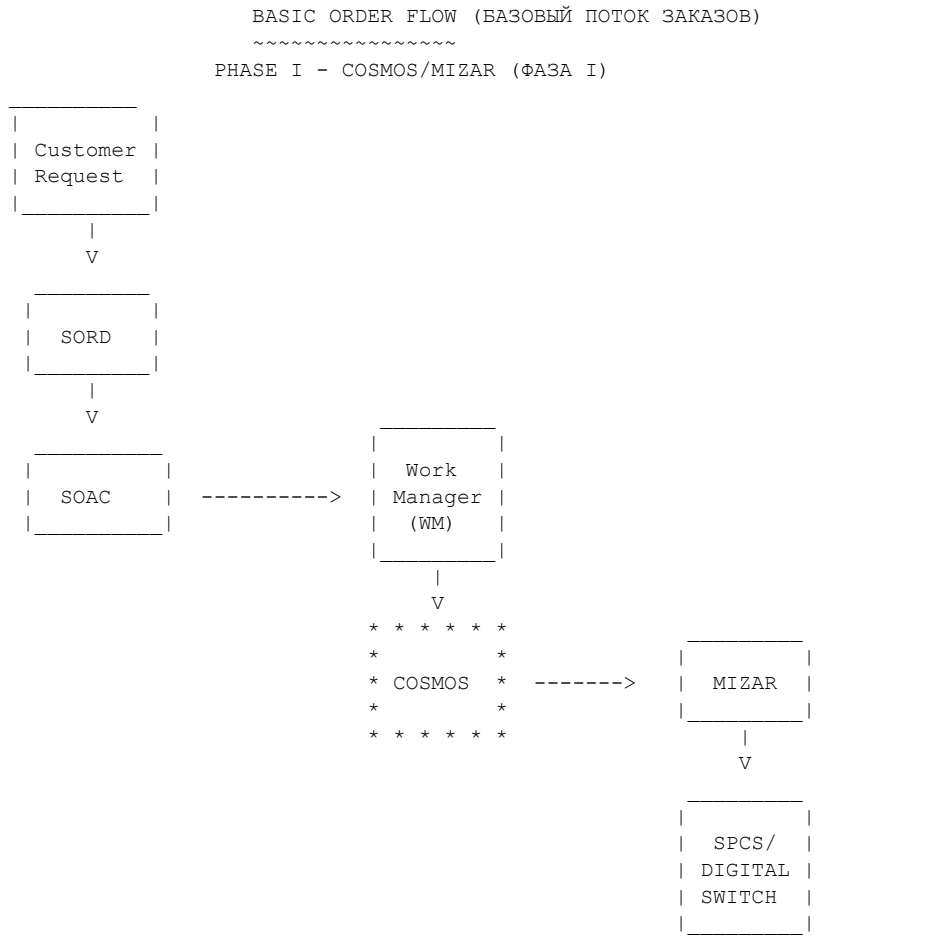
LFACS — Loop FACS содержит весь инвентарь петлевых объектов и отвечает на запросы о назначении.

COSMOS — COmputer System for Mainframe OperationS содержит весь инвентарь OE и отвечает на запросы OE.

SORD — Service ORder and Distribution (Распределение сервисных заказов) распределяет Сервисные Заказы по всей системе.

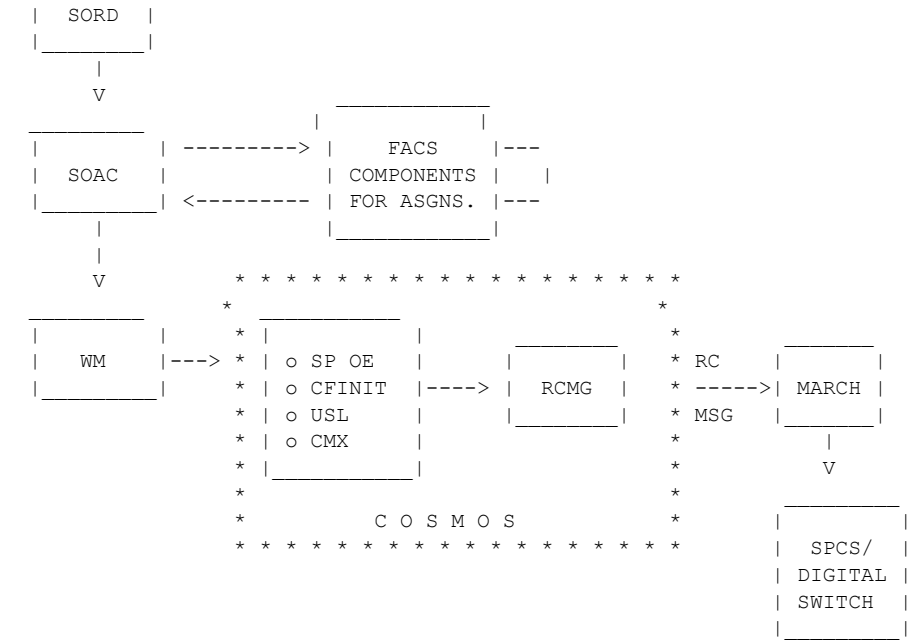
MARCH — MARCH является обновлением MIZAR, которое вступает в игру при модернизации Stromberg-Carlson (SxS и XBAR) до Generic 17.1 (программный интерфейс называется NAC). Хотя существует проблема с интерфейсом между MARCH и COSMOS (поскольку Generic Interface не поддерживается COSMOS), для MAN, AGE, LETS и т.д. используются шаблоны. В любом случае, MARCH играет большую роль в этой системе. MARCH, помимо упомянутого выше, выполняет базовую функцию поддержания RCMAC в актуальном состоянии по коммутаторам

(пользовательская транзакция MSR). Это менеджер RC-сообщений, позволяющий изменять сообщения (ORE), просматривать данные использования (MAR) и ведущий журнал всех передач.



... И появился MLAC

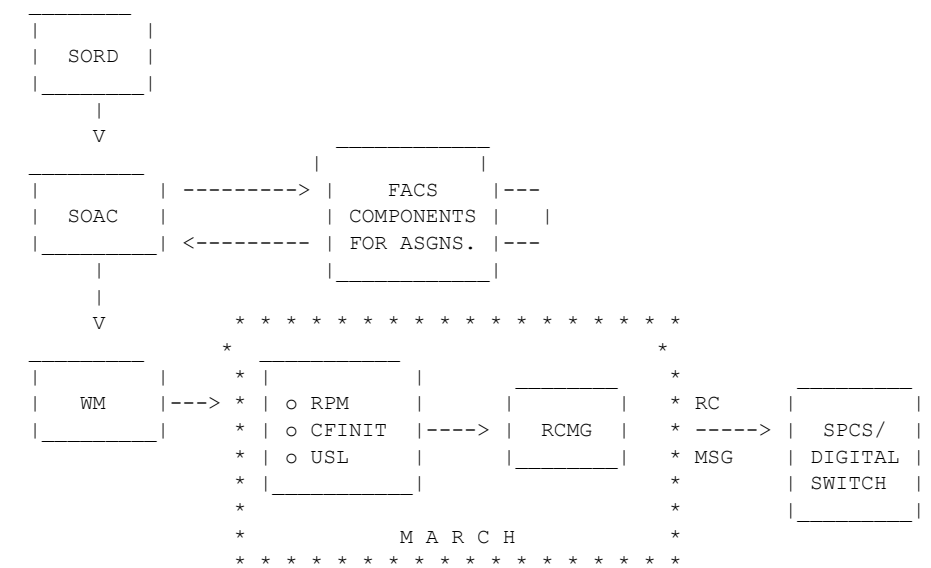
С переходом на FACS ввод данных, ранее осуществлявшийся вручную LAC и NAC, был заменён механизированным потоком данных от SOAC к COSMOS (через Work Manager). Таблицы, используемые для Recent Change (CFINIT, USL и CXM) и резервные назначения OE хранятся в COSMOS вместе с генератором RC-сообщений (RCMG). LAC и NAC теперь задействуются только в исключительных случаях (это будет подробнее объяснено позже).



... ТЕПЕРЬ ЕСТЬ SOAC/MARCH

В конфигурации SOAC/MARCH (конфигурация FACS/MARCH) основным источником данных о сервисных заказах по-прежнему остаётся SOAC. COSMOS выводится из сферы Recent Change в этом приложении (за исключением, как и LAC с NAC, отдельных случаев) и становится просто ещё одним компонентом FACS. Таблицы, находившиеся в COSMOS или Recent Change, теперь продублированы в MARCH.

Вместо получения, хранения и передачи уже отформатированных RC-сообщений MARCH теперь сам генерирует Recent Change из данных, переданных из SOAC, — так же как ранее делал COSMOS.



E. Подготовка к сообщениям об изменениях

НАЧАЛО С SORD

Сервисные Заказы (SORD) содержат FID и USOC (Universal Service Order Codes — Универсальные коды сервисных заказов [эти коды указывают тип услуги, которую клиент может иметь или получить]) с данными, специфичными для запроса на обслуживание клиента (SORD обращается к PREMIS для получения телефонного номера и данных адреса; другие записи вносятся Представителем по обслуживанию). Затем заказ передаётся в SOAC.

ЗАТЕМ В SOAC

SOAC использует внутренние таблицы для чтения FID и USOC, переданных SORD, чтобы определить, какая информация требуется от различных компонентов FACS. Затем SOAC обращается к соответствующим компонентам FACS (LFACS для назначения кабельных пар; COSMOS для назначения OE) и собирает необходимые данные.

После сбора всех данных SOAC передаёт информацию в Work Manager. Данные передаются либо как есть, либо SOAC (снова используя внутренние таблицы) переводит их в формат, приемлемый для принимающих систем (то есть COSMOS и MARCH).

SOAC передаёт информацию, предназначенную для MARCH, одним из двух способов:

TP-Flow-Through Translation Packets (Пакеты трансляции TP)

Пакеты трансляции (TP) содержат полностью транслируемые данные, из которых MARCH может генерировать RC-сообщение. Определение осуществляется SOAC на основе возможностей интерфейса и его способности читать, транслировать при необходимости и передавать данные.

Service Order Image (Образ сервисного заказа)

Образы Сервисных Заказов отправляются в MARCH, если SOAC не может передать все необходимые данные. Образы требуют дополнительной информации, вводимой вручную или извлекаемой из COSMOS, до генерации RC-сообщений.

WORK MANAGER — РЕГУЛИРОВЩИК ТРАФИКА

Основная функция Work Manager — читать сервисный заказ и определять, куда должны быть отправлены данные. Решения включают:

Система COSMOS	Система MARCH
Wire Center COSMOS	Коммутатор MARCH
Control Group COSMOS	Обслуживающая RCMA

Work Manager передаёт данные сервисного заказа в MARCH в режиме реального времени (заказы, которые ранее удерживались в COSMOS до запроса по Frame Due Date [FDD], теперь хранятся в MARCH), либо в виде TP, либо в виде образа.

1. Когда MARCH получает пакет трансляции (TP)

(1) Пакет трансляции, переданный из SOAC через Work Manager, принимается в MARCH программой CIP (Communication Interface Program — Программа коммуникационного интерфейса).

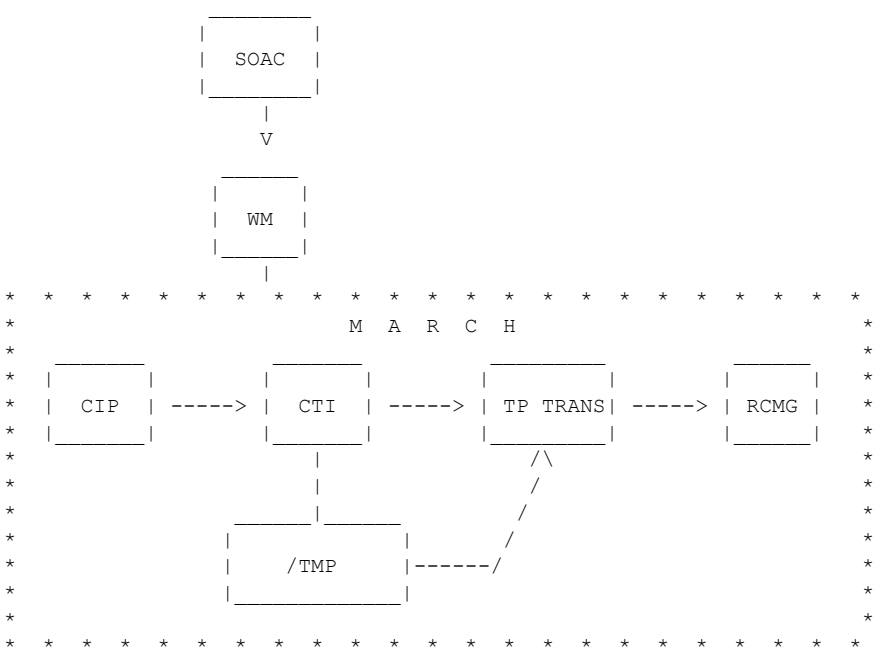
(2) Когда данные получены CIP, он вызывает CTI или модуль управления заданиями (Job Control Module). Job Control Module или CTI записывает полученные данные во временный файл и сообщает TP Trans (Translation Translator — Транслятор трансляций), что заказ получен. Также контролирует количество одновременно выполняемых заданий, переданных в TPTrans.

(3) TPTrans анализирует заказ во временном файле, выполняет соответствующее преобразование FID (например, удаление тире), переформатирует заказ и передаёт его в генератор RC-сообщений (RCMG).

(4) RCMG выполняет всю генерацию RC-сообщений и после завершения записывает заказ в ожидающий файл MARCH (Pending Header или Review file).

В дополнение к данным, переданным из SOAC, RCMG использует следующие данные в MARCH для трансляции в сообщения, приемлемые для коммутатора:

```
NXX                 Switch Specific Parameters (RPM)
USOC (RPM)          CCF Keywords (CFINIT)
USOC/NXX (RPM)      Review Triggers (RVT)
                    Release Times (SRM)
```



2. Когда MARCH получает образ сервисного заказа

(1) Образ Сервисного Заказа, переданный из SOAC через Work Manager, принимается в MARCH программой CIP (Communication Interface Program).

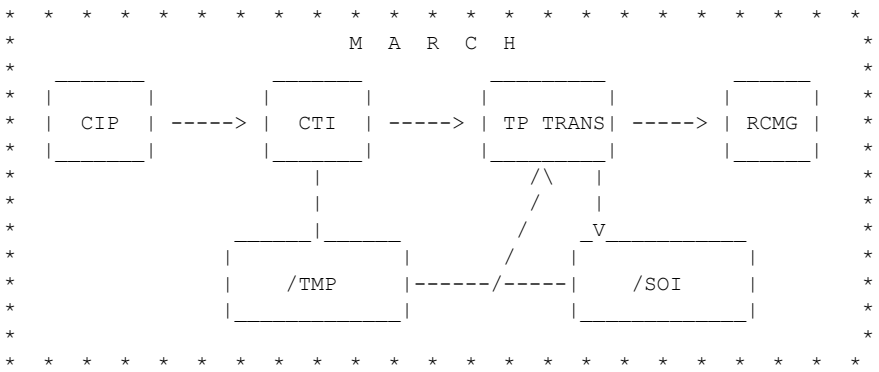
(2) Когда образ получен CIP, он вызывает CTI или Job Control Module. Job Control Module или CTI записывает полученные данные во временный файл и сообщает TP TRANS (Translation Translator), что заказ получен. Также контролирует количество одновременно выполняемых заданий, переданных в TPTrans.

(3) TP TRANS анализирует заказ во временном файле, определяет, что это образ сервисного заказа, и создаёт файл SOI (Service Order Image) с использованием номера заказа и имени файла. Весь образ записывается в файл SOI. TP TRANS сигнализирует программе SOIP (Service Order Image Processor) для дальнейшей обработки.

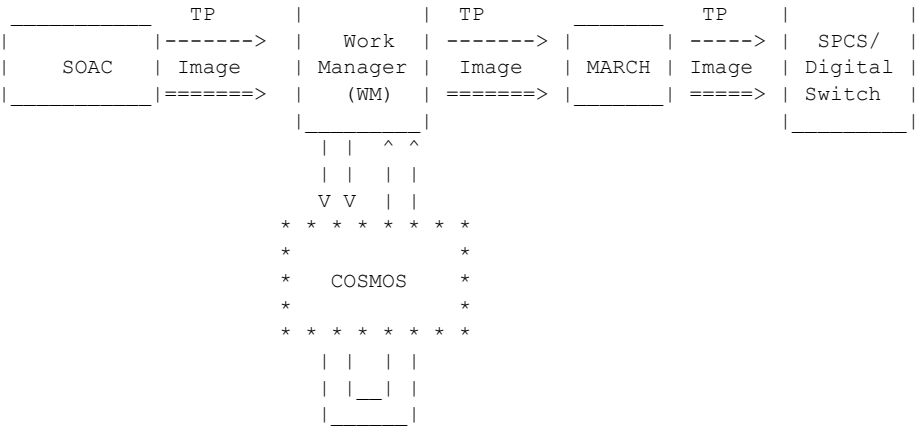
(4) Если SOIP может определить коммутатор, для которого предназначен образ, он передаёт запрос в файл Call COSMOS и сохраняет данные образа в файле IH (Image Header). Если SOIP не может определить коммутатор, образ помещается в PAC (Unknown Switch Advisory) для ручной обработки.

(5) Для образов, коммутатор которых определён, MARCH обращается к COSMOS в следующее запланированное время вызова и запускает RCP по номеру заказа (если последнее время вызова прошло, запрос откладывается до первого времени вызова следующего дня).

(6) Если заказ получен из COSMOS, он помещается в файл PH или RV соответствующим образом, и Image Header удаляется. Устанавливается флаг, указывающий, что в системе существует текст образа Сервисного Заказа. Если заказ не получен из COSMOS, образ помещается в PAC для ручной обработки.



Вам не обязательно знать все программы, которые MARCH использует для обработки Сервисных Заказов в среде SOAC/MARCH. Это становится тривиальным и запутывается в различных командах, которые ничего не значат, если только вы, конечно, не работаете с данной системой.



Хотя понять работу всех этих систем довольно трудоёмко, ниже представлен краткий обзор MARCH. Для охвата MARCH сначала рассмотрим фоновую обработку.

F. Фоновая обработка в MARCH

RECENT CHANGE PARAMETER (RPM)

В сочетании с шаблонами ORI и шаблонами Recent Change, RPM определяет, как информация из SOAC изменяется и/или обрабатывается для создания приемлемых RC-сообщений коммутатора.

Руководитель RCMA несёт общую ответственность за RPM. Хотя отдельные категории могут поддерживаться Staff Manager, в целом ответственность лежит на RCMAC.

Это включает данные преобразования Line Class Code (LCC), ранее находившиеся исключительно под ответственностью NAC в COSMOS. Требуется изменение процедур для RCMA, чтобы обеспечить передачу правильной информации LCC в RPM и своевременное её обновление.

Начальные данные преобразования USOC в LCC будут скопированы в MARCH из таблицы USOC COSMOS.

SWITCH RELEASE MANAGER (SDR)

В конфигурации SOAC/MARCH он больше не определяет типы заказов, извлекаемых из COSMOS, и устанавливает дату и время выпуска заказов на коммутатор — поступающих как из SOAC, так и из COSMOS.

Основан на Package Type (PKT) и Package Category (PKC).

ТРАНЗАКЦИЯ SWINIT

Содержит специфические для коммутатора данные, необходимые MARCH для связи с SOAC (через Work Manager), COSMOS и коммутатором.

Устанавливает время вызовов для COSMOS:

• RCP по номеру заказа для образов Сервисных Заказов.
• Приостановки, восстановления и отключения за неуплату.
• Автоматические запросы AGE (при применимости).
• Автоматический отчёт MAN.

SDR — SWITCH DATA REPORT (Отчёт о данных коммутатора)

SDR — транзакция отчёта, предназначенная для использования сотрудником RCMA.

Switch Data Report предоставляет распечатку информации SWINIT, заполненной из Анкеты подготовки, поданной Руководителем RCMA (см. часть «Описание заказа» этого файла).

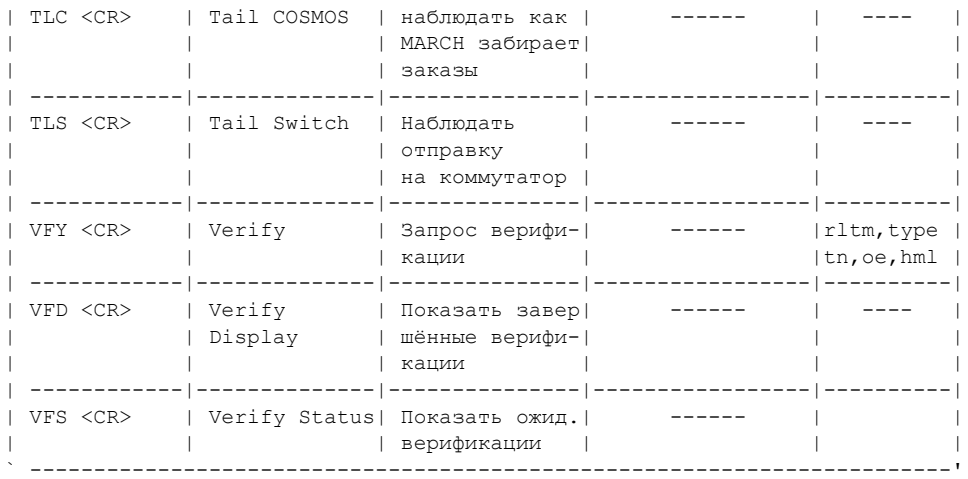
MOI заказа в истории

Заказы в файле History Header (HH) отражают источник истории. Источник истории показывает, как заказ был записан в файл истории.

G. Пользовательские транзакции в MARCH

Наиболее часто используемые команды MARCH

Транзакция	Название	Функция	Ключи поиска	Подсказки
MSR <CR>	MARCH Status Report	статус офиса	. <CR> sw address	----
MOI <CR>	MARCH Order Inquiry	статус заказа, tn, файла	fn rv fn rj fn hh/adt xx-xx so n12345678 tn xxxxxxx	----
ONC <CR>	On Line COSMOS	Доступ COSMOS	------	login password
ONS <CR>	On Line Switch	Доступ к коммутатору	------	Switch logon
ORE <CR>	Order Edit	Редакт. загол. или текста файла MARCH	fn rv fn rj so n12345678 tn xxxxxxx	----
ORE -G <CR>	Order Edit Global	глобал. ред. нескольких файлов	2 ключа поиска обязательны	----
ORI <CR>	Order Input	Создать файл MARCH	------	Patterns
ORS <CR>	Order Send	Отправить на коммутатор немедленно	so n12345678 tn xxxxxxx	----



Транзакция	Название	Функция	Ключи поиска	Подсказки
MSR <CR>	MARCH Status	статус офиса	. <CR>	----
	Report		sw address	
MOI <CR>	MARCH Order	статус	fn rv	----
	Inquiry	заказа, tn,	fn rj	
		файла	fn hh/adt xx-xx	
			so n12345678	
			tn xxxxxxx	
ONC <CR>	On Line	Доступ COSMOS	------	login
	COSMOS			password
ONS <CR>	On Line	Доступ к	------	Switch
	Switch	коммутатору		logon
ORE <CR>	Order Edit	Редакт. загол.	fn rv	----
		или текста	fn rj	
		файла MARCH	so n12345678	
			tn xxxxxxx	
ORE -G <CR>	Order Edit	глобал. ред.	2 ключа поиска	----
	Global	нескольких	обязательны	
		файлов		
ORI <CR>	Order Input	Создать файл	------	Patterns

		MARCH		
ORS <CR>	Order Send	Отправить на	so n12345678	----
		коммутатор	tn xxxxxxx	
		немедленно		
TLC <CR>	Tail COSMOS	наблюдать как	------	----
		MARCH забирает		
		заказы		
TLS <CR>	Tail Switch	Наблюдать	------	----
		отправку		
		на коммутатор		
VFY <CR>	Verify	Запрос верифи-	------	rltm,type
		кации		tn,oe,hml
VFD <CR>	Verify	Показать завер	------	----
	Display	шённые верифи-		
		кации		
VFS <CR>	Verify Status	Показать ожид.	------	
		верификации		

Подробное описание некоторых команд:

MOI — MARCH ORDER INQUIRY (Запрос заказа MARCH)

MOI — диалоговая транзакция запроса, предназначенная для использования клерком RCMAC.

MOI используется для запроса RC-сообщений в ожидающем файле (файлах): Pending Header, Review, Reject и/или History Header. Может использоваться для запроса одного сообщения, всего заказа, нескольких сообщений из более чем одного файла или всех заказов в файле — в зависимости от введённых ключей поиска.

ONS — ON line Switch (Онлайн коммутатор)

Каждый коммутатор имеет собственную последовательность входа.

```
DMS-100
   Вход
   1) Выдать аппаратный разрыв (Hard Break)
   2) На приглашении "?" набрать "login"
   3) Появится приглашение "Enter User Name". Ввести имя пользователя.
   4) Затем "Enter Password" со строкой из @, *, & и #, скрывающей пароль.
   5) После входа набрать "SERVORD" — вы окажетесь на RC-канале коммутатора.

   Выход
```

```
   1) Набрать "LOGOUT" и CONTROL-P

1AESS
   Вход
   1) Включить Echo, Line Feeds и Caps Lock.
   2) Завершать каждое VFY-сообщение " . CONTROL-D", а каждое RC-сообщение
      "! CONTROL-D".

   Выход
   1) Нажать CONTROL-P

5ESS
   Вход
   1) На приглашении "<" набрать "rcv:menu:apprc".

   Выход
   1) Набрать "Q" и нажать CONTROL-P
```

ONC — On Line COSMOS

```
1) Вы увидите "login:", введите имя пользователя; затем появится
   приглашение "Password:" для ввода пароля.
```

ORE — Order Edit (Редактирование заказа)

Команды ORE используются для перемещения между окнами и к предыдущим и последующим заголовкам и тексту в рамках сеанса редактирования. Команды могут вводиться в любой точке сеанса ORE независимо от положения курсора. Это заглавные буквы, требующие использования клавиши Shift, или управляющие команды. Вот команды перемещения:

```
Команда              Описание
~~~~~~~~             ~~~~~~~~~~~
N (ext header)       Заменяет данные на экране следующим заголовком и
                     связанным текстом, соответствующим введённым ключам
                     поиска.
M (ore text)         Заменяет данные в окне текста сообщения следующим
                     сообщением, связанным с текущим заголовком (для
                     сообщений с несколькими текстами).
P (revious header)   Заменяет данные в окнах заголовка заголовком,
                     просмотренным ранее (в том же сеансе редактирования).
B (ackup text)       Заменяет данные в окне текста сообщения текстом,
                     просмотренным ранее (в том же сеансе редактирования).
S (earch window)     Перемещает курсор в окно поиска, позволяя ввести
                     дополнительные ключи поиска.
Control-D            Следующая страница
Control-U            Предыдущая страница
<                    Переместить курсор из окна текста в заголовок.
>                    Переместить в окно текста из заголовка.
Q (uit)              Выход
```

ORE -G

ORE -G — диалоговая транзакция, предназначенная для использования сотрудником RCMA.

ORE -G используется для глобального редактирования RC-сообщений в ожидающем файле MARCH: Pending Header, Review и Reject. Возможности редактирования включают добавление информации к заказу.

ORE -G также используется для изменения информации заголовка и удаления сообщений.

ORI — ORder Input (Ввод заказа)

Ввод заказа позволяет вводить заказ и изменять заказы. Изменения можно вносить в телефонный номер, OE и т.д. Эта команда слишком сложна, чтобы подробно рассматривать её здесь.

VFY — Verify (Верификация)

Используется для ручного ввода сообщений верификации в MARCH, а затем на коммутаторы.

MSR — MARCH Status Report (Отчёт о состоянии MARCH)

Используется для подсчёта количества сервисных заказов, хранящихся в SOAC. Также показывает количество сообщений об изменениях, отправленных на коммутатор.

H. Формы сервисных заказов

За время работы мне встречалось множество распечаток, которые поначалу были совершенно непонятны. Спустя несколько месяцев я начал разбираться в некоторых кодах. Вот некоторые распространённые сервисные заказы и их назначение.

Сервисный заказ SORD:

```
 _____________________________________________________________
|                                                             |
|TN           CUS TD     DD     APT MAC ACC AO    CS  SLS     HU  |
|415-343-8765 529 T      DUE    W           AS OF 1FR ABCDE4W     |
|ORD       SU   EX     STA APP CD     IOP CT TX RA SP CON AC      |
|C14327658      SMIUX      R              R                       |
|ACNA  R                                                        |
|WA    343# EXETER,SMT                                          |
|WN    IDOL, BILLY                                              |
|---S&E                                                         |
|I1    ESL                                                      |
|O1    1FR/TN 343-8321/ADL                                      |
|      /PIC 10288                                               |
|O1    ESL/FN 3438321                                           |
|---BILL                                                        |
|MSN   IDOL, BILLY                                              |
|MSTN  555-1212                                                 |
|---RMKS                                                        |
|RMK   BLAH                                                     |
|                                                               |
|      /**** END                                                |
|_____________________________________________________________|
```

```
 _____________________________________________________________
|[1]          [2]       [3]                      [9]            |
| |            |         |                        |             |
|TN           CUS TD     DD     APT MAC ACC AO    CS  SLS     HU  |
|407-343-8765 529 T      DUE    W           AS OF 1FR ABCDE4W     |
|                                                               |
| [8]                                                           |
|  |                                                            |
| ORD       SU   EX     STA APP CD     IOP CT TX RA SP CON AC     |
|C14327658      SMIUX      R              R                      |
|ACNA  R                                                        |
|                                                               |
|[4]                                                            |
| |                                                             |
|WA    343# EXETER,SMT                                          |
|                                                               |
|[6]                                                            |
| |                                                             |
|WN    AT&T                                                     |
|---S&E                     \                                   |
|I1    ESL                  |                                   |
|O1    1FR/TN 343-8321/ADL  | [5]                               |
|      /PIC 10288           |                                   |
|O1    ESL/FN 3438321       /                                   |
|---BILL                                                        |
|                                                               |
|  [6]                                                          |
|   |                                                           |
|  MSN   IDOL, BILLY                                            |
```

```
|                                                                  |
|  [7]                                                             |
|   |                                                              |
|  MSTN  555-1212                                                  |
|---RMKS                                                           |
|RMK   BLAH                                                        |
|                                                                  |
|      /**** END                                                   |
|__________________________________________________________________|
```

- **[1]** Телефонный номер. Формат XXX-XXX-XXXX.
- **[2]** Номер клиента.
- **[3]** Дата исполнения.
- **[4]** Рабочий адрес.
- **[5]** Поле S&E:

КОД ДЕЙСТВИЯ — это код в крайнем левом столбце страницы. Коды заканчиваются на 1 или 0. 1 означает добавить эту функцию, 0 — не выполнять функцию. Существует несколько различных кодов действий:

Код действия	Применение
I	Добавить функции
O	Удалить функции
C-T	Изменить назначенное количество звонков, номер "переадресации" или оба параметра для функций переадресации при занятости/задержке.
E-D	Ввести или удалить функцию только для записей.
R	Сводка CCS USOC для уведомления

Список некоторых распространённых USOC (функций):

ESC	Трёхсторонний вызов (Three Way Calling)
ESF	Быстрый набор (Speed Calling)
ESL	Быстрый набор 8 кодов (Speed Calling 8 Code)
ESM	Переадресация вызовов (Call Forwarding)
ESX	Ожидание вызова (Call Waiting)
EVB	Переадресация при занятости (Busy Call Forward)
EVC	Расширенная переадресация при занятости
EVD	Отложенная переадресация вызовов
HM1	Intercom Plus
HMP	Intercom Plus
MVCCW	Commstar II Call Waiting

- **[6]** Имя для выставления счёта
- **[7]** Номер для выставления счёта
- **[8]** Номер сервисного заказа
- **[9]** Класс обслуживания или LCC

Информация заголовка файла SDR (MARCH)

1. Название коммутатора
2. Имя файла заголовка
3. Текущая дата и время
4. Номер сервисного заказа
5. Тип сервисного заказа
6. Телефонный номер
7. Тип пакета
8. Категория пакета
9. Причина отклонения
10. Дата и время выпуска
11. Дата и время принятия
    Дата и время отклонения
12. Источник ввода

Файл истории заголовка (History Header File)

```
       [1]                    [2]                    [3]
        |                      |                      |
       sw: swad0             history header file     fri may 31 07:50:12 1992

[4]-  so=janet3                    tn=         pkt-in     pkc=other
[11]- act=05-30 0750   src=ori      |           |          |
      history text=      |         [6]         [7]        [8]
```

```
       rc:sclist:        [12]
       ord 31235
       cx =031235
       adn 2
       ! ~
```

Файл отклонений (Reject File)

```
  [1]-  sw:swad2       [2]- reject file   [3]- fri may 30 11:22:01 1992

   [4]- so=c238          [5]- ver=7  tn=5551212  -[6]
   [9]- rj reason=ot    rldt=05-30 1059   rjdt=05-30 :106 src=cosmos
        message test=    |                 |               |
        rc:line:chg:    [10]              [11]            [12]
        ord 87102
        "=238-7102'
        "ord c231"
        "restoration from ssv-db"
        tn 555 1212
        lcc 1mr
        ! ~
        ve data=
          , er

        m 07 rc18 0 87102 0 4 valar
             new 00001605 err 00000307
             05/30/92 11:07:16
```

I. Сервисный заказ COSMOS из команды SOI

```
 _____________________________________________________________________
|WC%                                                                  |
|WC% SOI                                                              |
|H ORD N73322444                                                      |
|                                                                     |
|             DEC 19, 1992   10:12:21 AM                              |
|           SERVICE ORDER ASSIGNMENT INQUIRY                          |
|                                                                     |
|ORD N733224444-A             OT(NC)      ST(AC- )       FACS(YES)    |
|   DD(12-20-92) FDD(12-20-92) EST(11-16:14) SG(G)  DT(XX   ) OC(COR)  |
|   MDF WORK REQ(YES) MDF COMPL(NO) LAC COMPL(NO) RCP(NO)             |
|   WPN 9446 WLST 1= P  2=     3=     4=    5=    6=     7=    8=     |
|   COORDINATION REQUIRED                                             |
|   RMK   FAT TBCC,RO D77901070                                       |
|   RMK   FAT TBCC,RO D77901070                                       |
|CP  48-0942                                                          |
|     ST SF   PC     FS WK   DATE 11-28-89   RZ 13                    |
|     LOC PF01008                                                     |
|OE 012-25-006                                                        |
|     ST SF PC       FS WK   DATE 11-12-91   CZ 1MB    US 1MS    FEA TNNL|
|     PIC 10288                                                       |
|     LCC BB1                                                         |
|     CCF   ESX                                                       |
|     LOC PF01007                                                     |
|TN   571-5425                                                        |
|     ST WK  PD FS WK  DATE 12-03-91    TYPE X                        |
|   **ORD D77901070-C       OT CD  ST AC-     DD 12-20-92  FDD 12-20-92  |
|                                                                     |
|** SOI COMPLEATED                                                    |
|WC%                                                                  |
|_____________________________________________________________________|
```

- **[1]** Дата и время запроса SOI в COSMOS
- **[2]** Заголовок выходного сообщения
- **[3]** Номер заказа

• **[4]** Тип заказа
• **[5]** Статус заказа
• **[6]** EST (11-16:14) — когда Сервисный Заказ был зарегистрирован в COSMOS
• **[7]** Дата исполнения
• **[8]** Frame Due Date (Дата исполнения монтажа)
• **[9]** Группа сегментов
• **[10]** Требуется ли работа на Главном распределительном фрейме
• **[11]** Завершена ли работа на Главном распределительном фрейме
• **[12]** Выполнено ли Loop Assignment Center
• **[13]** FACS Y — заказ загружен из SOAC в MARCH; RCP N
• **[14]** Телефонный номер
• **[15]** Текущее состояние телефонного номера
• **[16]** Будущий статус телефонного номера
• **[17]** Дата последней активности по телефонному номеру
• **[18]** Тип телефонного номера
• **[19]** Линейное оборудование
• **[20]** Текущий статус линейного оборудования
• **[21]** Будущий статус телефонной линии
• **[22]** Дата последней активности по линейному оборудованию
• **[23]** Класс обслуживания
• **[24]** USOC
• **[25]** Функции
• **[26]** Функция пользовательского вызова (Custom Calling Feature)
• **[27]** Код класса линии (Line Class Code)
• **[28]** Тип заказа, закрывающего телефонный номер
• **[29]** Статус заказа, закрывающего телефонный номер
• **[30]** Дата исполнения
• **[31]** Frame Due Date
• **[32]** Расположение линейного оборудования на фрейме
• **[33]** Кабельная пара
• **[34]** Текущий статус кабельной пары
• **[35]** Будущий статус кабельной пары
• **[36]** Дата последней активности по кабельной паре
• **[37]** Зона сопротивления
• **[38]** Номер заказа, закрывающего кабель
• **[39]** Расположение кабельной пары на фрейме
• **[40]** Сообщение о завершении SOI
• **[41]** Wire Center и символ приглашения, указывающий на готовность компьютера к следующей транзакции
• **[42]** Первичный независимый перевозчик — 10288 (Ten Triple X код AT&T)

J. MSR — Отчёт о состоянии MARCH

```
 ____________________________________________________________________
|                                                                    |
|  switch name                                                       |
|  ==================================================================|
|                          march status report                       |
|      sw:switch name                    tue oct 30 11:14:48 1992    |
|                       pending work functions                       |
|  ==================================================================|
```

```
|                          past due         due today       future due   |
|  ____________________________________________________________________  |
|  use moi for:               0                 0                 0      |
|  reject file                0                 1               270      |
|  review file                0                 0                 0      |
|  held release status       28                14                44      |
|  normal release status      0                 7               184      |
|  ____________________________________________________________________  |
|  use pac for:               0                15                        |
|  change notices             0                 3                        |
|  unknown switch notices     0                 0                        |
|  ====================================================================|
|                                                                        |
|  ** msr completed                                                      |
|________________________________________________________________________|
```

- **[1]** Офисный MSR-запрос по (имя/адрес коммутатора)
- **[2]** Дата и время запроса
- **[3]** Колонка просроченных сервисных заказов
- **[4]** Просроченные сервисные заказы на удержании
- **[5]** Колонка сервисных заказов со сроком сегодня
- **[6]** Заказы со сроком сегодня в файле отклонений
- **[7]** Заказы со сроком сегодня в файле проверки
- **[8]** Заказы со сроком сегодня на удержании
- **[9]** Заказы со сроком сегодня с нормальным статусом выпуска
- **[10]** PAC-сервисные заказы, которые были изменены
- **[11]** Уведомления о переключении PAC, поступившие сегодня
- **[12]** Колонка сервисных заказов с будущим сроком
- **[13]** Заказы с будущим сроком с нормальным статусом выпуска

K. Прочие замечания

LCC, или Line Class Code (Код класса линии), — это, коротко говоря, тип линии, который может иметь абонент Bell. Это идентификаторы типа телефонной линии. Эти идентификаторы используются SCC (Switching Control Center) и коммутаторами для определения типа выставления счёта. Вот список некоторых распространённых LCC, используемых стандартным BOC. Примечание: это не высечено в камне. Они могут варьироваться от района к району.

```
1FR  - One Flat Rate (Единый фиксированный тариф)
1MR  - One Measured Rate (Единый тарифицируемый звонок)
1PC  - One Pay Phone (Один таксофон)
CDF  - DTF Coin (Монетный DTF)
PBX  - Private Branch Exchange (Прямой входящий набор, внутр. АТС)
CFD  - Coinless ANI7 Charge-a-Call (Безмонетный ANI7)
INW  - InWATS
OWT  - OutWATS
PBM  - 0 HO/MO MSG REG (No ANI)
PMB  - LTG = 1 HO/MO Regular ANI6
```

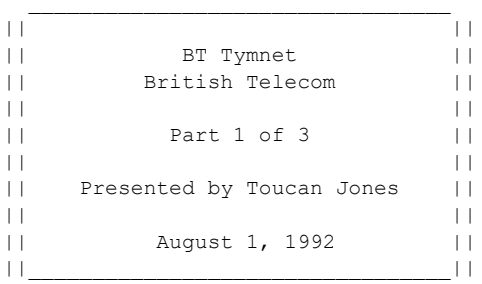
L. Рекомендуемая литература

- Файл Agent Steal в LODTJ #4
- Acronyms 1988 [c Metal Shop Private BBS] (Phrack 20, File 11)
- «Lifting Ma Bell's Cloak Of Secrecy» by VaxCat (Phrack 24, File 9)

BT Tymnet / British Telecom. Часть 1 из 3

Автор: Toucan Jones

1 августа 1992 г.



> *«Мы сыграли ключевую роль в том, чтобы первыми обнаружить их присутствие.»*
>
> *«Если вы посмеете ковыряться в нашей сети и мы вас поймаем — а мы всегда ловим — вы поплатитесь за это.»*

— Джон Гинассо, директор по глобальной сетевой безопасности дочерней компании Tymnet, BT North America, в журнале Information Week (13 июля 1992 г., стр. 15).

Добро пожаловать в Tymnet!

ЧАСТЬ 1
• A. Индекс точек доступа BT Tymnet
• B. Доступ к BT-GNS через региональные телефонные компании Bell
1. Bell Atlantic
2. BellSouth
3. Pacific Bell
4. Southwestern Bell
5. Southern New England Telephone
• C. Базы данных и компании, работающие в режиме разделения времени на Tymnet
• D. Классификация услуг для баз данных и компаний, использующих Tymnet
• E. Сводная таблица глобальных сетевых услуг по странам
• F. Идентификаторы терминалов
• G. Параметры входа в систему

ЧАСТЬ 2
• H. Служба глобального асинхронного набора исходящих соединений BT-GNS

ЧАСТЬ 3
• I. Глобальный доступ BT-GNS, отсортированный по узлам

A. Индекс точек доступа BT Tymnet

Country	Abbrev.	Country	Abbrev.
ANTIGUA	ATG	HONG KONG	HKG
ARGENTINA	ARG	ISREAL	ISR
AUSTRALIA	AUS	ITALY	ITA
AUSTRIA	AUT	JAMAICA	JAM
BAHAMAS	BHS	JAPAN	JPN
BAHRAIN	BHR	KOREA	KOR
BARBADOS	BRB	NETHERLANDS	NLD
BELGIUM	BEL	NORTHERN MARIANAS	SAP
BERMUDA	BMU	PANAMA	PAN
CANADA	CAN	PERU	PER
CAYMAN ISLANDS	CAY	PHILIPPINES	PHL
COLUMBIA	COL	PURERTO RICO	PRI
DENMARK	DNK	SWEDEN	SWE
DOMINICAN RPUBLIC	DOM	SWITZERLAND	CHE
EGYPT	EGY	TRINIDAD AND TOBAGO	TTO
FRANCE	FRA	UNITED KINGDOM	GBR
GREECE	CRC	URUGUAY	URY
GUAM	GUM	USA	USA
GUATEMALA	GTM	VIRGIN ISLANDS	VIR
HONDURAS	HND	WEST GERMANY	DDR

B. Доступ к BT-GNS через региональные телефонные компании Bell

Сеть TYMNET имеет шлюзы во многие пакетные сети региональных телефонных компаний Bell. Подробная информация о порядке доступа к этим сетям приведена в конце настоящего раздела.

[Таблица из ~160 записей — узлы доступа BT-GNS по городам США с номерами дозвона — опущена]

```
B=BELL 103/113 (300 bps) или BELL 212A (1200 bps) — совместимые модемы
C=CCITT V.21 (300 bps) или CCITT V.22 bis (2400 bps) или CCITT V.32 —
  совместимые модемы.
```

B1. Bell Atlantic

```
@PDN  BELL ATLANTIC — НАЗВАНИЕ СЕТИ: PUBLIC DATA NETWORK (PDN)

      (СООБЩЕНИЕ О ПОДКЛЮЧЕНИИ)
      ...<CR>            (СИНХРОНИЗАЦИЯ СКОРОСТЕЙ ДАННЫХ)

      WELCOME TO THE BPA/DST PDN

      *.T <CR>           (АДРЕС TYMNET)


      131069             (ПОДТВЕРЖДЕНИЕ АДРЕСА — DNIC TYMNET)
      COM                (ПОДТВЕРЖДЕНИЕ УСТАНОВКИ СОЕДИНЕНИЯ)

      -GWY 0XXXX- TYMNET: PLEASE LOG IN:  (НОМЕР ХОСТА В СКОБКАХ)
```

B2. BellSouth

```
@PLSK  BELLSOUTH — НАЗВАНИЕ СЕТИ: PULSELINK

      (СООБЩЕНИЕ О ПОДКЛЮЧЕНИИ)
```

```
        ... <CR>            (СИНХРОНИЗАЦИЯ СКОРОСТЕЙ ДАННЫХ)
                            (НЕ ОТОБРАЖАЕТСЯ НА ТЕРМИНАЛЕ)
        CONNECTED
        PULSELINK

        13106               (АДРЕС TYMNET)
                            (НЕ ОТОБРАЖАЕТСЯ НА ТЕРМИНАЛЕ)

        PULSELINK: CALL CONNECTED TO 1 3106

        -GWY 0XXXX- TYMNET: PLEASE LOG IN:  (НОМЕР ХОСТА В СКОБКАХ)
```

B3. Pacific Bell

```
  @PPS   PACIFIC BELL — НАЗВАНИЕ СЕТИ: PUBLIC PACKET SWITCHING (PPS)

        (СООБЩЕНИЕ О ПОДКЛЮЧЕНИИ)

        ...<CR>             (СИНХРОНИЗАЦИЯ СКОРОСТЕЙ ДАННЫХ)
                            (НЕ ОТОБРАЖАЕТСЯ НА ТЕРМИНАЛЕ)

        ONLINE 1200
        WELCOME TO PPS:  415-XXX-XXXX
        131069              (АДРЕС TYMNET)
                            (НЕ ОТОБРАЖАЕТСЯ ДО ОТВЕТА TYMNET)

        -GWY 0XXXX- TYMNET: PLEASE LOG IN:  (НОМЕР ХОСТА В СКОБКАХ)
```

B4. Southwestern Bell

```
  @MRLK - SOUTHWESTERN BELL TELEPHONE — НАЗВАНИЕ СЕТИ: MICROLINK II(R)

        (СООБЩЕНИЕ О ПОДКЛЮЧЕНИИ)
        (PLEASE TYPE YOUR TERMINAL IDENTIFIER)

        A                   (ВАШ ИДЕНТИФИКАТОР ТЕРМИНАЛА)

        WELCOME TO MICROLINK II
        -XXXX:01-030-
        PLEASE LOG IN:
        .T <CR>             (ИМЯ ПОЛЬЗОВАТЕЛЯ ДЛЯ ДОСТУПА К TYMNET)


        HOST: CALL CONNECTED

        -GWY 0XXXX- TYMNET: PLEASE LOG IN:
```

B5. Southern New England Telephone

```
  @CONNNET - SOUTHERN NEW ENGLAND TELEPHONE — НАЗВАНИЕ СЕТИ: CONNNET

        (СООБЩЕНИЕ О ПОДКЛЮЧЕНИИ)

        HH<CR>                  (СИНХРОНИЗАЦИЯ СКОРОСТЕЙ ДАННЫХ)
                                (НЕ ОТОБРАЖАЕТСЯ НА ТЕРМИНАЛЕ)
        CONNNET

        .T<CR>                  (ТОЛЬКО ЗАГЛАВНЫЕ БУКВЫ)
        26-SEP-88   18:33       (ДАТА)
```

```
        031069                  (ПОДТВЕРЖДЕНИЕ АДРЕСА)
        COM                     (ПОДТВЕРЖДЕНИЕ УСТАНОВКИ СОЕДИНЕНИЯ)

        -GWY OXXXX-TYMNET: PLEASE LOG IN:
```

C. Базы данных и компании, работающие в режиме разделения времени на Tymnet

• APCUG "GLOBALNET" BBS
• Bloodstock Research Information
• BRS Information Technologies
• BT, North America (Dialcom)
• Cartermill, Inc.
• Charles Schwab and Company, Inc.
• Chemical Abstracts Services (CAS)
• Commercial SABRE
• Commodity Systems, Inc.
• CompuServe, Inc.
• Compusource
• Computer Intelligence
• Connect, Inc.
• Creative Automation Co.
• Delphi
• Dialog Information Services, Inc.
• Digital Equipment Corp.
• Diversified Network Applications, Inc.
• Dow Jones & Company, Inc.
• Dun and Bradstreet
• Electronic Data Systems Corp.
• Export Network, Inc.
• Gibson Information Systems (GIS)
• Global Interconnect Communications, Inc.
• Idioma Translation
• Interactive Data Corp.
• Jeppesen DataPlan
• Mead Data Central
• Metro On-Line Services, Ltd.
• National Library of Medicine (NLM)
• NewsNet, Inc.
• Nikkei Telecom Japan
• Nuclear Power Experience
• OCR Services, Inc.
• Official Airline Guide (OAG)
• ORBIT Search Service
• Power Computing Company
• Rand McNally — TDM, Inc.
• Real Estate Investment Network
• SeniorNet
• Southeast Regional Data Center (SERDAC)

• SPEED>S Corporation
• The Jockey Club Information Systems
• TRW Business Credit Division
• TRW Information Services
• USA TODAY Sports Center
• West Publishing Company (WEST)
• Xerox Computer Services (XCS)

D. Классификация услуг для баз данных и компаний, использующих Tymnet

ОСНОВНЫЕ КАТЕГОРИИ:

Бизнес	Инвестиции
Коммуникации	Право
Компьютеры	Животноводство
Экономика	Маркетинг
Образование	Медицина
Электронная почта	Природные ресурсы
Экология	Недвижимость
Финансы	Безопасность
Игры	Наука
Общие интересы	Спорт
Государственное управление	Торговля
Здравоохранение	Транспорт
Страхование	Путешествия
Международные темы	

ПРОЧИЕ КАТЕГОРИИ:

Государственное управление	Торговля
Здравоохранение	Транспорт
Страхование	Путешествия
Международные темы	

Глобальная сетевая служба BT TYMNET (GNS) объединяет три уровня международных услуг:

1. **BT TYMNET GLOBAL NETWORK CONNECTION SERVICE** (Служба глобального сетевого подключения BT TYMNET)
2. **ENHANCED GLOBAL CONNECTION SERVICE** (Расширенная служба глобального подключения)
3. **BASIC GLOBAL CONNECTION SERVICE** (Базовая служба глобального подключения)

СЛУЖБА ГЛОБАЛЬНОГО СЕТЕВОГО ПОДКЛЮЧЕНИЯ BT TYMNET (TGN) в настоящее время предоставляется в следующих странах:

• Австралия
• Бельгия
• Канада
• Дания
• Франция
• Германия
• Италия
• Япония
• Нидерланды
• Новая Зеландия
• Испания
• Швеция
• Швейцария
• Великобритания
• США

Объекты и оборудование службы BT TYMNET GLOBAL NETWORK CONNECTION SERVICE принадлежат и управляются компанией BT TYMNET. Глобальная, региональная и местная поддержка обеспечивается end-to-end квалифицированным техническим персоналом BT TYMNET, работающим по всему миру с 1977 года. Предусмотрена круглосуточная служба приёма сообщений о неисправностях и реагирования на критические проблемы. Доступны расширенное ценообразование, выставление счетов в местной валюте и выставление счетов конечным пользователям.

РАСШИРЕННАЯ СЛУЖБА ГЛОБАЛЬНОГО ПОДКЛЮЧЕНИЯ (EGC) дополняет описанную выше службу и в настоящее время доступна из следующих мест:

• Аляска (США)*
• Антигуа
• Аргентина
• Австралия
• Австрия
• Багамы
• Бахрейн
• Барбадос
• Бельгия
• Бермуды
• Каймановы острова
• Дания
• Доминиканская Республика
• Франция
• Германия

• Гуам*
• Гватемала
• Гондурас
• Гонконг
• Израиль
• Италия
• Ямайка
• Корея
• Нидерландские Антильские острова
• Панама
• Перу
• Филиппины
• Пуэрто-Рико*
• Саудовская Аравия
• Швеция
• Швейцария
• Тортола
• Тринидад и Тобаго
• Великобритания
• Виргинские острова США

* Применяются внутренние тарифы и условия обслуживания США

Служба ENHANCED GLOBAL CONNECTION SERVICE предоставляется местными телекоммуникационными администрациями, оснащёнными технологиями BT TYMNET. Во многих случаях администрация использует сетевых супервайзеров BT TYMNET для управления пакетным сервисом в своём регионе.

Все точки ENHANCED GLOBAL CONNECTION SERVICE обеспечивают прямое подключение по проприетарному протоколу TYM2 к публичной сети BT TYMNET и, таким образом, могут предоставлять широкий спектр расширенных протокольных услуг BT TYMNET. Большинство из них в настоящее время предлагают асинхронный доступ BT TYMNET и сервис X.25. Благодаря тесным отношениям между BT TYMNET и провайдерами ENHANCED GLOBAL CONNECTION SERVICE в этих точках обеспечивается высокий уровень обслуживания и поддержки. Из всех указанных мест доступна услуга TYMUSA — универсальный коммутируемый доступ с выставлением счетов на домашний офис клиента.

БАЗОВАЯ СЛУЖБА ГЛОБАЛЬНОГО ПОДКЛЮЧЕНИЯ (BGC) завершает полный спектр международного подключения и в настоящее время доступна из следующих мест:

• Антигуа, Аргентина, Австралия, Австрия, Багамы, Бахрейн, Барбадос, Бельгия, Бермуды, Бразилия, Канада, Каймановы острова, Чили, Китай, Колумбия, Коста-Рика, Кюрасао, Кипр*, Дания, Джибути*, Доминиканская Республика, Египет, Фарерские острова*, Финляндия, Франция, Французские Антильские острова, Французская Гвиана, Французская Полинезия*, Габон, Гамбия, Германия, Греция, Гренландия*, Гваделупа*, Гуам и Сайпан, Гватемала, Гондурас, Гонконг, Венгрия, Исландия, Индия, Индонезия, Ирландия, Израиль, Италия, Берег Слоновой Кости, Ямайка, Япония, Кувейт, Люксембург, Макао*, Мадагаскар, Малайзия, Мальта*, Маврикий*, Мексика, Мозамбик*, Намибия, Нигер, Нидерланды, Нидерландские Антильские острова*, Новая Каледония*, Новая Зеландия, Северные Марианские острова, Норвегия, Панама, Перу, Филиппины, Португалия, Пуэрто-Рико, Катар, Реюньон, Сан-Марино*, Саудовская Аравия, Сенегал*, Сингапур, Южная Африка, Южная Корея, Испания, Швеция, Швейцария, Тайвань, Таиланд, Тортола (Британские Виргинские острова)*, Тринидад и Тобаго, Тунис*, Турция, Острова Тёркс и Кайкос*, ОАЭ, Виргинские*

острова США, Вануату, Великобритания, США, Уругвай, СССР, Югославия*, Зимбабве

* Информация будет доступна в следующем обновлении

Провайдеры BASIC GLOBAL CONNECTION SERVICE подключают свои сети к BT TYMNET исключительно через шлюзы по протоколу X.75. Рекомендация CCITT X.75 тесно связана с более известной рекомендацией CCITT X.25 и обеспечивает надёжный канал связи для взаимодействия между публичными сетями передачи данных.

Являясь поставщиком сетевых технологий для американских IRC и зарубежных операторов на протяжении более 10 лет, компания BT TYMNET располагает богатым опытом работы со стандартом X.75 и активно участвует в его развитии. Программное обеспечение BT TYMNET X.75 превратилось в сложный продукт с многочисленными расширенными функциями, не встречающимися в других реализациях X.75. BT TYMNET поддерживает и обслуживает больше шлюзов X.75, чем любая другая сеть в мире.

Все шлюзы X.75 BT TYMNET обслуживаются группой International Network Services (INS) BT TYMNET, которая обеспечивает единообразную настройку всех шлюзов вне зависимости от сети-источника.

E. Сводная таблица глобальных сетевых услуг по странам

> *Примечание: TYMNET GLOBAL NETWORK (TGN) использует присвоенный BT TYMNET код DNIC 3106. Прочие коды DNIC, приведённые в таблице ниже, принадлежат провайдерам ENHANCED GLOBAL CONNECTION (EGC) и BASIC GLOBAL CONNECTION (BGC).*

[Таблица из ~180 записей — страны, DNIC, название сети, принадлежность к TGN/EGC/BGC — опущена]

F. Идентификаторы терминалов

Идентификатор терминала сообщает сети характеристики вашего терминала. Большинство терминалов могут использовать идентификатор «A». Однако если ваш терминал требует задержки возврата каретки, следует использовать идентификатор «I» или «E».

При появлении запроса `please type your terminal identifier` введите:

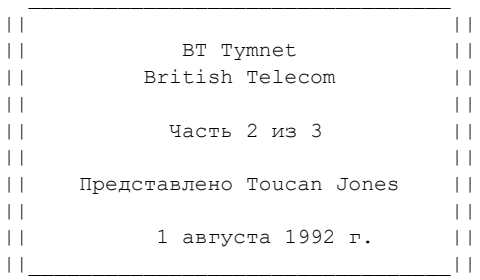
```
A  для ПК и CRT-терминалов (чётность SAVE)
C  для ударных принтерных терминалов на 300 бод
E  для термопринтерных терминалов типа SILENT 700
F  для транзакционных терминалов BETA
G  для GE Terminet на 1200 бод
I  для термопринтерных терминалов на 300 бод
K  для терминалов с чётным/нечётным контролем чётности (будущая реализация)
O  для терминалов с контролем чётности MARK/SPACE (доступ к BBS)
Y  для транзакционных терминалов на 300 бод
```

G. Параметры входа в систему

При появлении приглашения `please log in:` пользователь может задать управляющие символы для настройки сети под свои нужды. Например, если при подключении к базе данных данные поступают слишком быстро, можно применить обратное давление, набрав `^S`. Однако сеть отреагирует на эту команду только в том случае, если на этапе входа в систему был указан параметр `^R`.

```
^E    - Ctrl-E - Переход в режим полного дуплекса (будущая реализация)
^H    - Ctrl-H - Переход в режим полудуплекса — отключить эхо!
^I    - Ctrl-I - Построить оптимальную цепь для интерактивного трафика
^P    - Ctrl-P - Принудительная чётная чётность (EVEN Parity)
^R    - Ctrl-R - Включить обратное давление хоста X-on X-off
^U    - Ctrl-U - Принудительный перевод данных терминала в верхний регистр
^V    - Ctrl-V - Построить оптимальную цепь для объёмного трафика
^W    - Ctrl-W - Стереть ввод до последнего разделителя
^X    - Ctrl-X - Включить обратное давление терминала X-on X-off
^Z    - Ctrl-Z - Отключиться / Выйти из системы
ESC   - Escape - Отменить ввод и получить новое приглашение please log in
BREAK - Break  - Переключиться на PAD X.3 X.28 X.29 по CCITT (отдельные узлы)
```

BT Tymnet / British Telecom — Часть 2 из 3



Автор: Toucan Jones

Добро пожаловать обратно в Tymnet!

Содержание

H. Всемирный асинхронный сервис исходящей связи BT-GNS

Ниже приведена таблица узлов исходящей связи BT-GNS для США. В столбцах указаны: номер хоста (HOST), город (CITY), штат (ST), страна (CNTRY), плотность трафика (DENS), доступные скорости модемного соединения (300/1200/2400/9600 bps), код зоны (AREA CODE) и флаг MNP (M/N/P).

Обозначения скоростей:

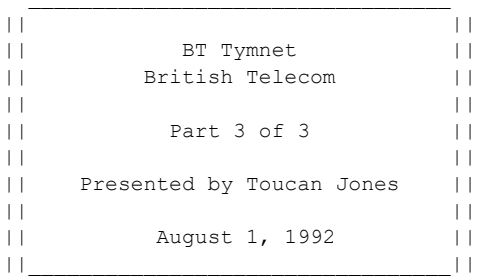
• **B** = модемы, совместимые с BELL 103/113 (300 bps) или BELL 212A (1200 bps)

• **C** = модемы, совместимые с CCITT V.21 (300 bps), CCITT V.22 bis (2400 bps) или CCITT V.32

[Таблица из 795 записей — опущена]

> ***Примечание переводчика:*** *Таблица содержит полный список узлов исходящей телефонной связи BT-GNS на территории США по состоянию на 1992 год. Записи охватывают все штаты — от Алабамы до Вайоминга — с указанием кодов городских телефонных зон, идентификаторов хостов сети и доступных скоростей передачи данных. Данные представляют исключительно историческую ценность: телефонные коды, названия местных операторов и сама сеть Tymnet претерпели значительные изменения после 1992 года.*

BT Tymnet / British Telecom — Часть 3 из 3



Автор: Toucan Jones

Дата: 1 августа 1992 года

С возвращением в Tymnet!

Содержание

I. Всемирный доступ BT-GNS, отсортированный по номерам узлов

Данный раздел представляет собой полную справочную таблицу точек коммутируемого доступа к сети Tymnet по всему миру, упорядоченную по номерам узлов. Таблица содержит следующие поля: номер узла (NODE), город (CITY), штат/провинция (ST), страна (CNTRY), плотность населённого пункта (DENS), поддерживаемые скорости дозвона в сотнях бит/с (300/1200/2400/9600), номер телефона для дозвона (ACCESS NO.), признак наличия MNP-сжатия (MNP) и примечания (COMMENTS).

[Таблица из ~1250 записей — опущена]

```
  NODE  CITY                 ST CNTRY DENS  3 12 24 96 ACCESS NO.   MNP COMMENTS
  ----- -------------------- -- ----- ----  ---------- ------------ --- --------
        Porto Alegre             BRA  BGC     C        (011) 15331  N   BGC Access
        Porto Alegro             BRA  BGC   C          (011) 15311  N   BGC Access
        Cartago                  CRI  BGC   C C        51-2000      N   BGC Access
        C. Quesada               CRI  BGC   C C        46-2000      N   BGC Access
        Heredia                  CRI  BGC   C C        38-2000      N   BGC Access
        Kuwait City              KUW  BGC   C          143          N   BGC Access
        Rio                      BRA  BGC     C        (021)2538153 N   BGC Access
        Cairo                    EGY  BGC   C          (2)3907102   N   BGC Access
        Sao Paolo                BRA  BGC   C          (011) 1531   N   BGC Access
  ...
  13655 Huntsville           AL  USA  MED   B B  C     205/882-1519 Y
```

Примечания к таблице

Узел 4003 используется для многих стран. Он представляет собой Enhanced Global Connection Service (Расширенную глобальную службу соединений), включающую узлы: 2576, 3512, 3513 и 4003.

Обозначения типов модемов:

• **B** — модемы, совместимые с BELL 103/113 (300 бит/с) или BELL 212A (1200 бит/с)
• **C** — модемы, совместимые с CCITT V.21 (300 бит/с), CCITT V.22 bis (2400 бит/с) или CCITT V.32

Обозначения скоростей в заголовке таблицы:

Позиция	Скорость
3	300 бит/с
12	1200 бит/с
24	2400 бит/с
96	9600 бит/с

Обозначения плотности населённого пункта (DENS):

• **HIGH** — крупный город
• **MED** — средний город
• **LOW** — малый город
• **WATS** — доступ через WATS (800-номер)
• **ALAS** — Аляска
• **CANH** — Канада (высокая плотность)
• **CANL** — Канада (низкая плотность)
• **BGC** — BGC Access (международные узлы)
• **E1/E2** — европейские узлы (класс 1/2)
• **PAC** — тихоокеанский регион
• **MX** — Мексика
• **HK** — Гонконг

Коды стран:

Код	Страна
USA	США
CAN	Канада
GBR	Великобритания
FRG	Германия (ФРГ)
FRA	Франция
NLD	Нидерланды
BEL	Бельгия
CHE	Швейцария
ITA	Италия
ESP	Испания
SWE	Швеция
DNK	Дания
IRL	Ирландия
GRC	Греция
TUR	Турция
POR	Португалия
AUS	Австралия
JPN	Япония
HKG	Гонконг
CHI	Чили
ARG	Аргентина
BRA	Бразилия
MEX	Мексика
CRI	Коста-Рика
EGY	Египет
KUW	Кувейт

SAU	Саудовская Аравия
UAE	ОАЭ
IND	Индонезия / Индия
MAL	Малайзия
THA	Таиланд
PHL	Филиппины
ISR	Израиль
IVC	Кот-д'Ивуар
CNA	Китай
GUM	Гуам
GTM	Гватемала
HND	Гондурас
JAM	Ямайка
NDA	Нидерландские Антильские острова
PAN	Панама
PRI	Пуэрто-Рико
TTO	Тринидад и Тобаго
VGB	Британские Виргинские острова
VIR	Виргинские острова (США)
ATG	Антигуа
CAY	Каймановы острова
ICE	Исландия
GIB	Гибралтар

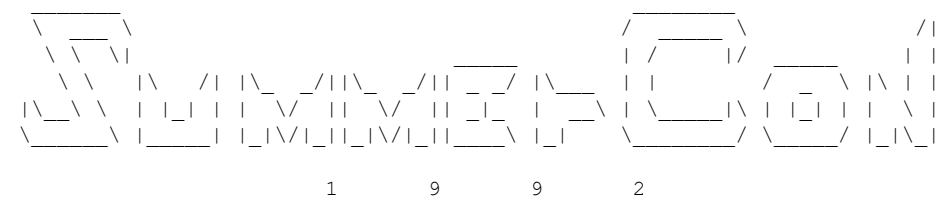
Код	Страна
USA	США
CAN	Канада
GBR	Великобритания

FRG	Германия (ФРГ)
FRA	Франция
NLD	Нидерланды
BEL	Бельгия
CHE	Швейцария
ITA	Италия
ESP	Испания
SWE	Швеция
DNK	Дания
IRL	Ирландия
GRC	Греция
TUR	Турция
POR	Португалия
AUS	Австралия
JPN	Япония
HKG	Гонконг
CHI	Чили
ARG	Аргентина
BRA	Бразилия
MEX	Мексика
CRI	Коста-Рика
EGY	Египет
KUW	Кувейт
SAU	Саудовская Аравия
UAE	ОАЭ
IND	Индонезия / Индия
MAL	Малайзия

THA	Таиланд
PHL	Филиппины
ISR	Израиль
IVC	Кот-д'Ивуар
CNA	Китай
GUM	Гуам
GTM	Гватемала
HND	Гондурас
JAM	Ямайка
NDA	Нидерландские Антильские острова
PAN	Панама
PRI	Пуэрто-Рико
TTO	Тринидад и Тобаго
VGB	Британские Виргинские острова
VIR	Виргинские острова (США)
ATG	Антигуа
CAY	Каймановы острова
ICE	Исландия
GIB	Гибралтар

Конец файла 10 из 14 — Phrack Inc., Том 4, Выпуск 40

«Я же говорил... Надо было прикончить меня в прошлом году!»



Автор: Knight Lightning & Dispater

Особая благодарность: Dr. Williams, Holistic Hacker, Nihil и The Pope

---

SummerCon '92

26–28 июня 1992 г.
Executive International Hotel

> *«SummerCon... Что это такое? Во многих отношениях SummerCon — это нечто большее, чем просто конвенция, собирающая величайших фрикеров и хакеров Америки. SummerCon — это состояние ума.*
> *Хакерам по природе своей свойственно скрытое чувство авантюризма: исследовать неизведанное, бросать вызов нетронутому, тянуться вперёд и экспериментировать со всем подряд. Осознание того, что ты не одинок в своём поиске, порой приходит как великий дар, а возможность встретиться со своими героями, партнёрами и кумирами может стать самым захватывающим моментом в жизни хакерского сообщества — вот о чём SummerCon.*
> *На поверхности SummerCon выглядит как кучка молодых людей, тусующихся в отеле в Сент-Луисе, штат Миссури. Для меня это скорее похоже на один из тех безумных фильмов, которые показывают поздно ночью по HBO или вроде того. Никакого особого смысла и направления, бунтари без причины — всё во имя бешеного веселья и игр. Атмосфера вокруг SummerCon — это атмосфера мира грёз, где раз в год можно сбежать в фантазию, где смекалка — король, а вокруг тебя в каждый момент есть друзья. Сам SummerCon длится лишь выходные, но дружба остаётся на всю жизнь.»*

— Knight Lightning, Phrack 28, File 8 (Специальный выпуск PWN о SummerCon '89)

SummerCon! Наконец-то — возвращение к исходной идее, лежавшей в основе этого события. Это было здорово! Это было безумно! Это была вечеринка! Это было всё, чем должно было быть, и даже больше.

Когда Taran King, Forest Ranger и Knight Lightning впервые задумали SummerCon в конце 1986 года, они, вероятно, и представить не могли, что все трое окажутся причастны к нему шесть лет спустя или что их идея, рождённая в школьные годы, станет настолько популярной.

Казалось, SummerCon '89 невозможно превзойти. Собрались 23 человека, состоялась серьёзная конференция, хватало всякого озорства и хаоса, и в целом все провели время отлично. В 1990 году

SummerCon по совпадению пришёлся на те же выходные, когда правительство США сняло обвинения с Knight Lightning. Народу пришло меньше десяти человек, и конференция никак не задалась.

В 1991 году SummerCon попробовал что-то новое. Темой того года стал CyberView с акцентом на вопросы гражданских свобод. Явка была средней, но чего-то не хватало. И наконец, в 1992 году дух SummerCon возродился заново.

Подготовка к SummerCon '92

Организация SummerCon в этом году оказалась делом непростым. Knight Lightning переехал в Вашингтон, округ Колумбия, Dispater жил не в Сент-Луисе, Taran King работал полный день, а Forest Ranger куда-то пропал. К счастью, был Rambone. При поддержке Taran King он взял на себя организацию гостиничного размещения и аренды конференц-зала, и без его помощи SummerCon вполне мог бы не состояться.

Нужно было уладить и множество других дел. Мы хотели, чтобы конференция этого года была особенной, и впервые решились на рискованное предприятие — разработку и продажу футболок Phrack/SummerCon. Knight Lightning и Dispater совместно работали над дизайном, а Dispater занимался художественным оформлением и производством. Для тех, кто не видел и не слышал об этих футболках, уместно дать краткое описание.

Футболки Phrack/SummerCon '92

Для конференции было изготовлено очень ограниченное количество футболок, и они были распроданы. Был сделан повторный заказ — в основном для тех, кто присутствовал на конференции, но не успел купить из-за малого тиража. Несколько штук отложили для людей, не сумевших приехать. В отличие от Legion of Doom с их туровыми футболками Internet World Tour, Phrack в настоящее время не планирует продавать футболки широкой публике. Если политика изменится, мы немедленно сообщим читателям.

Футболки стандартные, белые, с короткими рукавами, без кармана.

Спереди: на левой груди — рисунок, напоминающий Оливера Уэнделла Джонса (хакера из комикса «Bloom County»). Он машет мечом, стоя в эпицентре под прицелом снайперского прицела. По кругу над ним надпись «SummerCon '92», а под ним — «June 26-28 St. Louis, MO».

Сзади:

```
                PHRACK
            M a g a z i n e
                _____
          ______________
                _____

          When You Care Enough
        To Indict The Very Best

    PHRACK: 1     Secret Service: 0

             911's A JOKE!

       The information contained
     herein should not be disclosed
```

```
to unauthorized persons.  It is
meant solely for use by authorized
employees of the BELLSOUTH Corporation
or any of its subsidiaries.
```

Executive International Hotel... Больше не Best Western?

Все заинтересованные стороны решили вернуться туда, где проходили лучшие конференции, — в Executive International Best Western Hotel. Однако нас ждал сюрприз. Выяснилось, что Executive International больше не является Best Western: отель обанкротился. Хуже того, банк, забравший имущество за долги, тоже лопнул — иными словами, Executive International теперь принадлежал правительству Соединённых Штатов!

SummerCon начинается

Всего происходило так много и народу на конференции было так много, что дать подробный отчёт о событиях SummerCon попросту невозможно.

Knight Lightning приехал в четверг, а Dispater прилетел в пятницу ранним утром. Когда KL и TK прибыли в отель около 13:00, конференция уже шла вовсю: у входа стояли группы парней из Техаса и Бостона в футболках Phrack, уже обменивавшихся байками. Пожалуй, самым большим сюрпризом стало появление Doc Holiday — пригласить его никому не удалось, и изумлён был прежде всего Erik Bloodaxe.

Народ прибывал весь день, и по мере этого среди ветеранов прошлых SummerCon нарастало странное ощущение. Да, Tuc и Lex Luthor здесь не было, но в остальном это уже выглядело как воссоединение людей со всех предыдущих SummerCon.

Lucifer 666 носился с Control C; Disk Jockey разъезжал по барам в центре города вместе с Forest Ranger и Tom Brokaw; Erik Bloodaxe и Doc Holiday позвонили девушкам, с которыми познакомились на прошлогодней конференции. Всё происходило так стремительно, что за всем было не уследить — мы и не пытались. Просто веселились.

Около трети участников SummerCon отправились смотреть «Бэтмен возвращается» — после похода в кино на SummerCon '89 это казалось хорошей идеей. Другие расположились у бассейна, бродили по отелю и примыкающему офисному комплексу, а некоторые устроили набег на бесплатный фуршет в отеле Radisson неподалёку.

Вашингтонский контингент гостей SummerCon был доволен большую часть вечера сидеть в своих номерах и исследовать интернет-ресурсы Сент-Луиса. Кто-то ездил в мусорные рейды, кто-то шёл в бары за женским обществом, а кто-то засел в номере Restricted Data Transmissions (RDT) на хороший информационный обмен.

Тем временем несовершеннолетний хакер по имени Pyro (ну надо же, какой оригинальный ник) первым познакомился с гордостью и радостью Спрингфилда, Иллинойс. Обе молодые женщины утверждали, что им по 16 лет, и Pyro первым ощутил их зрелость. Одну из «девочек» звали Дена, и она явно была настроена на приключения. Цепляясь чуть ли не к каждому парню в отеле, она отказывалась уходить. В конце концов исчезла в чьём-то номере — и больше о ней не было слышно до следующего утра.

SummerCon: Конференция

Активности предыдущего вечера дали о себе знать. Когда наступил полдень, большинство хакеров ещё даже не проснулись, не говоря о том, чтобы быть готовыми к конференции. Заседание перенесли на 13:00, а пока Knight Lightning раздавал экземпляры Security Insider Report (от Interpact), материалы об InterTek, статью из ComputerWorld, написанную Крисом «Erik Bloodaxe» Гоггансом (эта статья также публикуется в PWN 40/1), тогда как Mr. Icom делал то же самое со старыми номерами Cybertek. Emmanuel Goldstein активно продавал новые чёрные футболки 2600 и раздавал старые номера журнала 2600. Среди материалов была и недавняя статья о хакерах, занимающихся компьютерной безопасностью, из Boston Business Journal — любезно предоставленная RDT. Кроме того, RDT был ответственен за изготовление кнопок SummerCon этого года. Holistic Hacker тоже сделал несколько. Спасибо всем причастным за отличную работу и усилия.

Хотя особо разглядеть её не давали, Knight Lightning с гордостью демонстрировал предрелизный экземпляр «THE HACKER CRACKDOWN» Брюса Стерлинга. Эта книга, которая поступит в продажу в твёрдой обложке 15 октября 1992 года, по всей видимости, станет одним из самых популярных литературных произведений о мире хакеров. В центре повествования — рейды в рамках дела Atlanta-LOD/Phrack/E911 и операции «Sun Devil». Есть основания полагать, что Knight Lightning сам изображён на обложке книги.

Ударив, как молотком, монтажной гарнитурой, Knight Lightning официально открыл заседание примерно в 13:15. Он выразил признательность за огромную явку — на заседании SummerCon присутствовало не менее 60 человек. Rambone вкратце прокомментировал события предыдущей ночи, вызвав взрыв смеха и шуток о «кибернимфах» со всех сторон зала.

Dispater на минуту взял слово, чтобы приветствовать всех гостей, и выразил благодарность членам RDT за помощь в выпуске Phrack в течение прошедшего года. Ненадолго разгорелась дискуссия о том, кому теперь принадлежит отель, а затем на трибуну был приглашён первый докладчик.

---

1. The Gatsby

«Уверен, вы все уже слышали в СМИ о «кольце из 1000 хакеров», якобы взламывающих кредитные бюро CBI/Equifax, — но эта история неправда, и за ней скрывается куда больше».

Gatsby объяснил, что хакер по имени The Prisoner (он же Multiplexor) из Индианаполиса (и отчасти, видимо, с Лонг-Айленда) прилетел в Сан-Диего к девушке — предположительно на купленный в карточку билет.

Находясь в Сан-Диего, он якобы взломал компьютеры ювелирного магазина Zale's и похитил данные кредитных карт из их системы торговых точек. Освободив снятую комнату, он опрометчиво оставил там распечатки с данными кредитных карт, и его бывший арендодатель (которому он задолжал деньги) их обнаружил и вызвал полицию Сан-Диего.

Несколько позже Multiplexor был встречен полицией в своём новом месте проживания — мотеле Sleepy Time в Сан-Диего. К делу подключилось ФБР, и его держали в отеле Marriott в течение двух недель за счёт государства! Находясь под правительственным надзором, Multiplexor входил в ряд систем, в том числе в Scantronics BBS.

В ходе расследования хакер по имени The Crypt Keeper пришёл к следователям, чтобы рассказать всё, что знал о хакерском подполье. В итоге он предоставил полиции доступ к журналам Scantronics

BBS, которые у него имелись, — он заходил в систему, используя пароль The Gatsby.

Эти журналы полиция использовала для получения ордеров на обыск у Scantronics BBS и у её теперь уже весьма недовольного бывшего сисопа Kludge.

[Полные подробности, полицейские отчёты, ордера и интервью с The Crypt Keeper опубликованы в Phrack World News 40/1.]

---

2. Agent Steal

Agent Steal прочёл весьма содержательный доклад о своих отношениях с Кевином Поулсеном, известным некоторым как Dark Dante. AS поделился частью переживаний и приключений, через которые они вдвоём прошли несколько лет назад, и рассказал о том, как Кевин ежедневно взламывал АТС. У Поулсена даже было специальное оборудование в квартире, чтобы помешать его прослушиванию. Поулсен, разумеется, стал фигурантом федерального обвинения и появился в одном из эпизодов «Нераскрытых тайн». С тех пор он был задержан и ожидает суда.

Сам Agent Steal провёл некоторое время в тюрьме по надуманным обвинениям, предъявленным с целью получить его содействие в преследовании Поулсена. Он отказался помогать, но в итоге всё равно был освобождён. Он сказал, что теперь с нетерпением ждёт чего-то нового — хотя, возможно, имел в виду концерт Оззи Осборна той ночью в Сент-Луисе. Agent Steal работает над книгой о своих приключениях с Поулсеном под названием «Data Thief» и рассчитывает выпустить её в ближайшем будущем.

---

3. Emmanuel Goldstein, редактор журнала 2600

«Многие люди не доверяют правительству и большому бизнесу и хотят знать, как дать им отпор».

Emmanuel Goldstein рассказал о Первой поправке и о том, почему журналу 2600 удавалось существовать и расти на протяжении многих лет, невзирая на события, обрушившиеся на Phrack в 1990 году. За восемь лет существования 2600 ни разу не подвергался прямым преследованиям со стороны властей. Главная причина, по его мнению, по которой Phrack попал под удар, а 2600 остался в покое, заключается в том, что 2600 — печатное (бумажное) издание.

Тем не менее 2600 нуждается в хороших авторах и готов публиковать что угодно — слитое или присланное напрямую, не важно. Против 2600 никогда не подавали иски, хотя угрозы судебным преследованием поступают регулярно [см. PWN 40/3 — последние угрозы в адрес 2600 со стороны Bellcore]. Подписка на 2600 составляет 1500 человек, а розничные продажи — 3000 экземпляров.

Он также рассказал о пресс-релизах, выпущенных с целью предупредить людей об уязвимых системах, — однако на эту информацию никто не реагирует, пока что-нибудь не случится. Людям всегда нравится винить журнал за то, что он объясняет, как что-то сделать (например, как открыть боксы FedEx), но никаких мер для устранения проблем, которые журнал выявляет, не предпринимается.

У Emmanuel было несколько вопросов от аудитории. Например, его спросили: «Как вы морально оправдываете хакинг и тип информации, публикуемой в 2600?» Он ответил, указав, что 2600 публикует только сведения об уязвимостях безопасности, которые необходимо изучить и устранить.

Emmanuel также спросили, были ли последствия от статьи о взломе замков Simplex — в ней описывалось, как без каких-либо инструментов менее чем за 20 минут (нередко менее чем за 3

минуты) вскрыть замок Simplex. Учитывая, что замки Simplex широко применяются в университетах и боксах FedEx, можно было ожидать каких-то мер. Emmanuel ответил, что сам был удивлён тем, что никакой реакции на статью не последовало. Однако, судя по тому, что ему рассказывали читатели, похоже, никто так и не поменял комбинацию по умолчанию!

---

4. Control C [Legion of Doom]

Control C — хакер, вокруг которого на протяжении многих лет крутилось немало противоречий: от его дней в Legion of Doom до трудоустройства и последующего увольнения из службы безопасности Michigan Bell.

Он рассказал об обстоятельствах, приведших его к работе в Michigan Bell. В 1987 году Control C начал почти ежедневно входить в компьютеры Michigan Bell — чтобы лучше освоить программирование на Си. В ходе одной четырёхчасовой сессии служба безопасности Michigan Bell отследила его звонок до Чикаго (где он тогда учился). На следующий день ^C вернулся в Детройт и получил звонок от неких господ, желавших пригласить его на обед.

Когда он явился, его встретили сотрудники службы безопасности Michigan Bell и шериф округа. Итогом стала работа, основной обязанностью по которой был поиск уязвимостей в компьютерной безопасности компании любыми доступными средствами. За эти годы Control C обнаружил более 100 различных дыр и иных слабых мест в их системах.

Со временем ключевые люди ушли, а им на смену пришли сотрудники с более консервативными взглядами; появился новый вице-президент (бывший полицейский), решивший, что держать хакера в штате больше не модно. Control C было предложено уйти, несмотря на то что необходимость в его услугах никуда не делась.

Вскоре после того, как Control C согласился уволиться, в дело вмешалась Секретная служба. Они хотели предъявить ^C обвинения за первоначальные взломы Michigan Bell, которые и привели к его найму. То, что Michigan Bell подписала документы об отказе от уголовного преследования, ничего не значило. Это не помешало Секретной службе взяться за него в 1990 году (в самый разгар дел E911/Phrack и LOD-Atlanta).

Control C предложили пройти проверку на детекторе лжи. Однако момент был неподходящий, и адвокат ^C добился переноса. Прошло уже более полутора лет с момента этого запроса, а ^C так и не получил никаких известий от Секретной службы. Сегодня ^C занялся новым делом.

---

5. Signal Surfer

Signal Surfer высказал свои опасения по поводу плохой репутации хакеров в компьютерной индустрии — притом что в реальности большинство людей в этой отрасли сами по себе хакеры. Он выразил желание объединить людей ради работы над изменением стереотипа о современном хакере и помощи хакерам в поиске легитимной работы в сфере IT.

---

6. Predat0r, редактор TAP Magazine; сисоп Blitzkrieg BBS

Predat0r коротко обновил информацию о текущем положении дел с TAP и попытался объяснить, почему больше года не выпускал ни одного номера. Виной тому были юридические проблемы

(связанные с обвинением в краже ноутбука), отнимавшие его время и ресурсы. Однако, по его словам, эти вопросы решены, и TAP возобновит выпуск с номера #106 где-то этой осенью.

Он пообещал, что не закроет журнал и не обманет всех, кто прислал ему деньги.

---

7. Mr. Icom, редактор Cybertek

Подобно Predat0r, Mr. Icom выразил сожаление о том, что несколько запоздал с выпуском новых номеров своего журнала. По его словам, номер #7 выйдет в ближайшее время.

---

8. Erik Bloodaxe (Chris Goggans) [Legion of Doom] [Comsec Data Security, Inc.]

Лишь год назад на SummerCon '91 Erik Bloodaxe, Doc Holiday и Malefactor с гордостью объявили о создании Comsec. И вот год спустя события, казалось, совершили полный круг. Что случилось с Comsec? Почему он прекратил работу? В чём дело? Это хотели знать все, и именно это Гоггансу предстояло обсудить.

Одним из факторов, повлёкших крах Comsec, стали операционные расходы на создание компании. Невыполненные обещания инвестиций со стороны таких людей, как Кеньон «Malefactor» Шульман, а также кампания слухов против них со стороны других игроков отрасли компьютерной безопасности и криминально небрежная пресса нанесли им тяжёлый удар — настолько тяжёлый, что оправиться не удалось.

Гогганс продолжил свой рассказ о коррупции и нечестной игре в сообществе безопасников. Так, было соглашение между Гоггансом и ISPNews о ведении им регулярной колонки в их двухмесячном издании. Однако после того как он сдал первую статью, вновь сформированный редакционный совет отказался её публиковать. Они заявили, что редсовет регулярно не допускает к публикации чувствительные материалы. Но когда ISPNews попросили назвать других авторов, чьи статьи прошли подобную проверку, — никаких имён не назвали. Стоит также отметить, что в состав редакционного совета входит некий Уильям Дж. Кук — бывший помощник прокурора США в Чикаго, тот самый обвинитель, которому принадлежат дела против соучредителя Phrack Крейга Нейдорфа (Knight Lightning), Shadow Hawk, Steve Jackson Games, Len Rose, The Mentor и самого Криса Гогганса!

Но это ещё не всё. Кто-то из редакционного консультативного совета (без разрешения Гогганса) переслал его статью руководителю службы безопасности SprintNet. Гогганс получил от SprintNet угрожающее письмо, в котором его статья называлась потенциально клеветнической, а также утверждалось, что она содержит неточности и конфиденциальную корпоративную информацию.

Но подождите: если статья содержит конфиденциальную информацию, то как она может быть неточной? А если она неточна, как она может раскрывать реальные уязвимости в системе безопасности?

Совсем недавно Гогганс написал статью для ComputerWorld (см. PWN 40/1) о хакерах и компьютерной безопасности. В ней рассматриваются проблемы безопасности Tymnet и Telenet: он разобрал, как хакеры эксплуатируют эти сети и как их можно остановить. Он зачитал статью вслух полностью. Она была типична для большинства материалов по безопасности — подробная, технически выверенная и несколько суховатая. Никаких громких откровений или советов по взлому.

Затем он зачитал некоторые редакционные ответы людей, отреагировавших на его статью в последующих номерах ComputerWorld. Аудитория их негативную реакцию не одобрила.

Наконец, разговор зашёл о ситуации с MOD. Гогганс рассказал о непрекращающихся преследованиях со стороны Phiber Optik и других членов его предполагаемой нью-йоркской организации.

По словам Гогганса, помимо обычных детских розыгрышей, которые ему регулярно устраивали, MOD получил его кредитную информацию, включая номера кредитных карт, и разместил её на BBS и в IRC. Они же изменили его домашний тарифный план с U.S. Sprint на AT&T, чтобы проще было получить его записи о звонках на дальние расстояния.

Он был не один — преследованиям подверглись и другие партнёры по Comsec, и мать Doc Holiday (Скотта Часина). Преследовать хакера — одно дело, но идти на семью и средства к существованию человека — это явно выходит за рамки хакерского кодекса этики. Нужно было что-то предпринять, и Comsec решил положить конец криминальной наглости MOD любыми доступными средствами.

Возникла дискуссия о надлежащем способе урегулирования ситуации. Гогганс признался, что в итоге обратился за помощью к ФБР, которое, к удивлению, оказалось весьма полезным. Часть участников SummerCon отнеслась к этому признанию критически.

Emmanuel Goldstein высказался наиболее откровенно: «Если мы начинаем просить ФБР решать наши проблемы, это худшее нарушение, чем то, что совершил MOD в отношении вас. Более уместной реакцией было бы использовать те же трюки, чтобы ответить им тем же».

Emmanuel привёл пример. Однажды в его офис посыпались звонки от людей, желающих приобрести туры в Европу. Оказалось, на автоответчике турагентства было оставлено исходящее сообщение, предлагавшее звонить и Джону Максфилду, и Эммануэлю Голдстейну с указанием обоих номеров. Максфилд решил проблему, обратившись к федералам... 2600 взломал автоответчик и заменил сообщение на что-то безобидное.

Какими бы остроумными ни были идеи Emmanuel, Гогганс заявил: «Законопослушные предприниматели не могут прибегать к незаконным методам для решения подобных ситуаций. У нас не было иного выбора».

Дискуссия продолжалась 30 минут, пока наконец Knight Lightning не вмешался, указав, что этот разговор может продолжаться вечно, и что пора заканчивать.

---

9. DrunkFux, директор HoHoCon

Прежде чем заседание официально завершилось, dFx хотел обсудить поведение гостей в отеле и поделиться историей с HoHoCon '91.

«Буйство на HoHoCon по сравнению со вчерашней ночью на SummerCon — это детский лагерь».

Drunkfux объяснил, что управляющие отеля HoHoCon обвинили гостей конференции во всевозможном ущербе и пригрозили возложить на dFx финансовую ответственность. Управляющий даже пригрозил снять деньги с его кредитной карты. dFx позвонил в свою компанию кредитных карт, и там ему сообщили, что угрозы отеля незаконны, а сами они были бы рады привлечь сеть Hilton к ответственности, если те попытаются выставить dFx подобный счёт.

Персонал Hilton утверждал, что кто-то из гостей конференции поджёг часть коридора, но отказался показать dFx место повреждений по его просьбе. Адвокат dFx (родственник, вмешавшийся к тому моменту) спросил, срабатывала ли пожарная сигнализация. Ответ был отрицательным. Тогда адвокат сообщил персоналу Hilton, что с удовольствием подаст на них в суд от имени гостей конференции за создание угрозы их жизни путём размещения в помещениях с неисправной пожарной сигнализацией. Персонал Hilton изменил показания.

Другое обвинение в адрес участников HoHo состояло в том, что они якобы распивали алкоголь и позволяли это делать несовершеннолетним. Адвокат указал, что именно барменам самого отеля пришлось обслуживать многих из них, и если утверждение Hilton соответствует действительности, он будет вынужден сообщить властям штата с целью отзыва лицензии на продажу алкоголя. Персонал Hilton изменил показания.

Эта последовательность «удар — ответный удар» повторялась ещё несколько раз, пока все претензии не были сняты.

Несколько дней спустя два управляющих отелем, ранее обвинявших dFx в ущербе, лично пришли к нему домой с извинениями. Они вручили ему купоны на бесплатное проживание при следующем посещении одного из их отелей. dFx записал встречу на видео и в шутку пообещал перевести запись в gif и раздать на ближайшей BBS!

После конференции

После официального заседания многие гости покинули отель — поесть, порыться в мусоре и исследовать город. Frosty и другие GCMS-MechWarriors затеяли партию в «Хакера» (Steve Jackson Games) в конференц-зале. Вскоре многие потянулись к торговому центру Northwest Plaza — где и началась очередная история.

Правило №4

Около десяти и более человек (в том числе Emmanuel Goldstein, The Conflict, Erik Bloodaxe, Doc Holiday и Signal Surfer) вошли в торговый центр Northwest Plaza, и у нескольких из них были бейсболки — козырьком назад.

Несколько минут спустя к ним подошла охрана торгового центра и сообщила, что ношение кепок задом наперёд нарушает Правило №4 и не допускается. Охранник сказал буквально следующее: «Вся одежда должна носиться так, как она предназначена для ношения». Логично: а разве кепки не предназначены для ношения на голове? Это было уже слишком для Emmanuel и остальных. Они прямиком направились в Sears, и Emmanuel купил всем (у кого ещё не было кепки) ярко-красные бейсболки St. Louis Cardinals.

Теперь у всех козырьки смотрели назад, и они принялись прогуливаться по торговому центру, вскоре привлекая внимание очередного бдительного охранника. После того как тот велел им развернуть кепки (и уронил рацию, пытаясь вызвать подкрепление), к нему подошёл Emmanuel, желавший обсудить это самое Правило №4.

Другой охранник невнятно пробормотал что-то о том, что дело по этому вопросу уже доходило до апелляционного суда, но об исходе умолчал, а подробностей нам так и не удалось найти.

Охранники (теперь в полном составе) сообщили Emmanuel, что это правило вывешено у всех входов, — и вытолкали всех из торгового центра. Emmanuel говорит, что обошёл весь торговый центр снаружи и убедился, что правило реально вывешено лишь у 2 из 12 входов. Ещё одно любопытное правило — №6, запрещавшее иметь в торговом центре сотовый телефон, пейджер или любое другое устройство, способное издавать звуки. Erik Bloodaxe нарушил это правило, сыграв на сотовом телефоне Signal Surfer «Мэри пасла ягнят».

Ночь

Ближе к позднему вечеру около половины участников Con отправились на набережную Сент-Луиса на Миссисипи (Laclede's Landing) — туда, где стоят прогулочные пароходы, работают бары и возвышается Арка.

Holistic Hacker показывал в своём номере видео:

• «ESS Phun» — юмористический набег трёх хакеров на центральную телефонную станцию Bell.
• «Unsolved Mysteries» — эпизод с Кевином Поулсеном.
• «Rudolph the Heavy-Metal Reindeer» — без комментариев.
• «Good Morning America» — смотрите, как Doc Holiday ПОЕДАЕТ собственную руку!
• «Now It Can Be Told» — Phiber Optik, Emmanuel Goldstein и Knight Lightning на шоу Гепальдо.
• «SummerCon '89» — лучшие моменты SummerCon '89.
• «SummerCon '91» — лучшие моменты SummerCon '91.

Ближе к вечеру всё вышло из-под контроля. Взрывались дымовые шашки, вырубался свет, комнаты заполнялись мусором, найденным в баках у крупных офисных зданий компьютерных и телекоммуникационных компаний. Дена снова вышла на охоту (и нашла жертву).

Agent Steal и DrunkFux отправились на концерт Оззи Осборна, тогда как Erik Bloodaxe и Doc Holiday ушли с девушками с прошлогодней конференции. Назад в отель они вернулись лишь следующим утром (и всем всё понятно).

Охранники носились по коридорам, угрожая посадить всех в тюрьму без конкретных причин, кроме как «за нарушение порядка».

Единственные серьёзные разговоры той ночью состоялись в номере RDT.

Воскресенье

Гости медленно просыпались незадолго до обязательного времени выезда из отеля. Когда они собирались в холле и на улице для последних разговоров и групповых фото, толпа постепенно редела. Некоторым нужно было сразу ехать в аэропорт, кто-то оставался до понедельника утром, но все пообещали вернуться на следующий год.

```
PWN ^*^ PWN ^*^ PWN { SummerCon '92 } PWN ^*^ PWN ^*^ PWN
PWN ^*^ PWN ^*^ PWN {  Guest List!  } PWN ^*^ PWN ^*^ PWN
```

Список гостей

Agent Steal Erik Bloodaxe The Not
Albatross Father Crime Omega
Apollo Phoebus Forest Ranger OPii
Aragorn Frosty Phaedrus
Black Phoenix Gateway Phantom Phreaker
Brian Oblivion The Gatsby The Pope
Bucky Golgo 13 Predat0r
The Butler Holistic Hacker The Public

Coder Decoder Hunter Pyro
Colin Junkmaster Rambone
The Conflict Just Dave Sarlo
Control C Knight Lightning Scooter
Count Zero Krynn The Serpent
Cray-Z Phreaker Lord MacDuff Signal Surfer
Crimson Death Louis Cypher Slack Master
Dark Angel Lucifer 666 Slave Driver
Dark Creaper Magic Man Taran King
Disk Jockey Minor Threat Tom Brokaw
Dispater Mr. Icom Video Vance
Doc Holiday Mucho Maas Voyager
Dr. Cypher Mudge Weapons
Dr. Williams Nat X White Knight
Drab Jester Night Ranger Wind Runner
Drunkfux Nihil
Emmanuel Goldstein Norris

Итого 73 человека — и именно они сделали всё это достойным воспоминания!

Несколько вещей, которые мы узнали на SummerCon

Автор: The Pope и Nihil

• Не пытайтесь покупать пиво в магазинах, у которых есть бензоколонки.
• Как правильно носить бейсболку.
• «Играть» на сотовом телефоне — незаконно.
• Все охранники торговых центров привезены из Миссисипи.
• Душ в Executive International работает только в двух режимах: ледяной и кипяток.
• Frosty закупил пожизненный запас гольф-носков до колена ещё до того, как они вышли из моды в 1970-х.
• Как знакомиться с несовершеннолетними девушками.
• Control C следовало выбрать псевдоним «No Control C».
• После 43 часов без сна (и 30 часов употребления алкоголя) акцент OPii исчезает.
• Тусоваться с Crimson Death и Phantom Phreaker — значит переживать в понедельник утром, не придётся ли сдавать анализ на наркотики на работе.
• Тусоваться с Crimson Death, Phantom Phreaker и Erik Bloodaxe научит вас, как пройти понедельничный тест на наркотики.
• Erik Bloodaxe и The Pope — это Сискел и Эберт мира порнофильмов.
• У Agent Steal пышная причёска.
• У Taran King идеальная причёска.
• НЕ садитесь в машину с Voyager и The Public.

BBS Scantronics захвачена полицейским управлением Сан-Диего — 1 июля 1992 года

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN               Phrack World News             PWN
PWN                                             PWN
PWN            Выпуск 40 / Часть 1 из 3         PWN
PWN                                             PWN
PWN         Составил Datastream Cowboy          PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Авторы: Knight Lightning и The Gatsby
Особая благодарность Брюсу Бигело (San Diego Union-Tribune)

> *«Multiplexor и The Crypt Keeper раскалываются»*

На протяжении последних двух месяцев в прессе циркулировало множество историй об ордах хакеров, похищающих данные кредитных карт и подрывающих экономику Соединённых Штатов. Всё началось со слухов о некоем Multiplexor'е — мелком хакере, который, по имеющимся сведениям, некоторое время провёл на Лонг-Айленде, штат Нью-Йорк, и, предположительно, родом из Индианы. По версии слухов, Multiplexor по краденой кредитной карте купил билет на самолёт до Сан-Диего — навестить девушку или встретиться с друзьями — но когда он приземлился, вместо знакомых его встретила полиция.

Откуда взялась эта информация или теория о «1000-членной хакерской группировке» — возможно, мы так и не узнаем. Однако благодаря полицейским рапортам и аффидавитам, предоставленным судом и добытым The Gatsby с помощью коллег, факты по этому делу нам теперь известны.

Эта и прочая информация стала доступна общественности.

Для понимания нижеследующего: «SEMENICK» и «MARCOV» — одно и то же лицо. Возможно, вы знаете его под никами Multiplexor или The Prisoner. Далее в этом файле встретятся упоминания некоего Кевина Маркуса, известного части сообщества как The Crypt Keeper.

Полицейское управление Сан-Диего — Дополнительный рапорт следователя

```
НОМЕР ДЕЛА: N/A
ДАТА:       23 марта 1992 года
ВРЕМЯ:      13:00
ТЕМА:       Оценка ущерба и сбор разведывательных данных о незаконном
            проникновении (хакерстве) в компьютерные системы и незаконном
            использовании кредитных карт.
ПОДОЗРЕВАЕМЫЙ: SEMENICK, John Edward  AKA: MARCOV, Eric Edward
ПОТЕРПЕВШИЙ:   Ювелирный магазин Zales
МЕСТО:      4465 La Jolla Village Drive, San Diego, CA
ДЕТЕКТИВ:   Dennis W. Sadler (уд. № 2486)
```

31 марта 1992 года я получил форму ARJIS 4 от офицера Смита (уд. № 3871) в отношении бумаг, обнаруженных неким господином Морисом Осборном у него дома.

Осборн попросил покинуть его жилище некоего Эрика МАРКОВА, снимавшего у него комнату. После ухода МАРКОВа Осборн обнаружил бумаги, на которых значилась информация, похожая на данные кредитных карт. Осборн позвонил в полицию и сообщил о находке.

Офицер Смит изъял бумаги и составил прилагаемый рапорт. Ознакомившись с документами, я установил, что они действительно содержат персональные данные ряда лиц — имя, адрес, номер кредитной карты, срок её действия и номер социального страхования. По всей видимости, тот, кто делал эти записи, незаконно использовал данные кредитных карт.

31 марта я связался с Осборном по телефону. Он подтвердил содержание рапорта и сообщил, что, по его мнению, МАРКОВ может всё ещё находиться в городе. 2 апреля со мной снова вышел на связь Осборн: он узнал, что МАРКОВ остановился в мотеле в пляжном районе под названием Sleepy Time.

2 апреля 1992 года, находясь в пляжном районе, я наткнулся на мотель Sleepy Time. Я обратился к администратору, Уильяму Гейнку, и спросил, не зарегистрирован ли у него постоялец по имени Эрик МАРКОВ. Тот подтвердил и уточнил, что МАРКОВ занимает номер 108.

Примерно в 8:40 я постучал в дверь номера 108. Дверь открыл белый мужчина. Я спросил, является ли он Эриком МАРКОВым. Он ответил утвердительно. Я представился детективом полиции Сан-Диего и сказал, что мне нужно поговорить с ним о сомнительных операциях с кредитными картами.

Когда он открывал дверь, я увидел на полу у входа бумаги, похожие на те, что передал мне Осборн, — с данными кредитных карт. Войдя в номер по приглашению, я спросил МАРКОВа, догадывается ли он о причине моего визита. Он ответил: «Думаю, да». На уточняющий вопрос пояснил: «Кредитные карты».

На тот момент я лишь брал у МАРКОВа показания в связи с бумагами, найденными у Осборна. Активного дела или каких-либо улик, указывающих на причастность МАРКОВа к уголовной деятельности, у меня не было.

Я спросил МАРКОВа, есть ли при нём документы, удостоверяющие личность. Он ответил отрицательно. МАРКОВ назвал следующие данные: Эрик Эдвард МАРКОВ, дата рождения 15.05.74, — затем поправился: 73-го. Сказал, что ему 18, скоро 19. Номера социального страхования он не помнил. На вопрос о водительских правах сообщил, что никогда их не имел. Внешне МАРКОВУ было от 17 до 19 лет.

В ходе разговора о бумагах он сам начал говорить о компьютерах и получении информации из различных систем. Говорил около десяти минут. После этого я решил уведомить ФБР, поскольку в получении данных кредитных карт было задействовано хакерство, а информация поступала из других штатов. Кроме того, МАРКОВ явно был хорошо осведомлён о компьютерном хакерстве и лично в нём участвовал.

В 8:58 я позвонил в местное отделение ФБР, изложил ситуацию и спросил, хотят ли они поговорить с МАРКОВым. Предварительно я спросил МАРКОВа, готов ли он беседовать с агентами ФБР о своей компьютерной деятельности. Он согласился.

Вскоре специальный агент Кит Мозес перезвонил мне в мотель. Я объяснил ему, что имею на руках, и что МАРКОВ готов говорить. Ознакомившись с делом, Мозес согласился приехать.

Мы с Мозесом вместе допросили МАРКОВа об его хакерской деятельности. МАРКОВ в течение последних четырёх лет был активно вовлечён в хакерское сообщество и располагал обширными знаниями о происходящем в хакерском мире. Позднее мы выяснили, что в начале 1991 года он был арестован по делу о компьютерных преступлениях в Индианаполисе. Мы пытались связаться со следователями по тому делу, однако, несмотря на многочисленные попытки, ответа так и не получили.

В ходе допроса я попытался установить подлинную личность МАРКОВа. Попросил данные его родителей. Он сказал, что не помнит их домашних телефонов, но телефон у них есть. Домашних адресов он тоже не помнил. На вопрос о месте работы родителей сообщил, что его отец работает в

местной (по месту жительства) компании, занимающейся турбинами.

Я позвонил в справочную местной телефонной компании, а затем — в саму фирму для проверки информации. Однако отдел кадров компании не обнаружил ни одного сотрудника с именем, которое назвал МАРКОВ. МАРКОВ также сообщил название своей школы и год выпуска. Звонок в административный отдел местного школьного округа показал, что никаких записей об обучении или выпуске МАРКОВа там нет.

Когда я предъявил ему эти факты, он наконец сообщил правдивые данные. Его настоящее имя — Джон Эдвард СЕМЕНИК, дата рождения 15.05.75. Я нашёл рабочий номер его отца и связался с ним. Тот был совершенно безразличен к местонахождению и состоянию сына. На вопрос, готов ли он оплатить авиабилет или автобус для возвращения сына домой, ответил отказом. Он добавил, что когда сын решит вернуться домой, то найдёт дорогу сам. Родители СЕМЕНИКа разведены, он живёт с отцом. Впрочем, выяснилось, что мать подала заявление о его побеге в местное шерифское управление.

Я связался с матерью — она проявила несколько большую озабоченность, однако также отказалась оплачивать билет или высылать деньги на обратный путь. Я спросил обоих родителей, будут ли они возражать, если, пока Джон находится в Сан-Диего, их сын окажет нам содействие в расследовании. Я объяснил, что в тот момент ему не предъявлено никаких известных уголовных обвинений, а предоставляемая им информация будет использоваться в целях оценки ущерба и сбора разведывательных данных о хакерах.

Оба родителя заявили, что не возражают против его содействия при условии отсутствия обвинений. Поскольку СЕМЕНИК являлся несовершеннолетним и по факту его побега было подано заявление, мы обратились за советом в прокуратуру США, в отдел по делам несовершеннолетних окружной прокуратуры и к дежурному офицеру учреждения для несовершеннолетних.

Нам сообщили, что препятствий для получения от него информации нет. СЕМЕНИК был помещён в учреждение для несовершеннолетних как беглец, а затем на ночь передан в переходный приют. Дежурный офицер пояснил, что, поскольку родители не готовы забрать его, его удержат лишь на одну ночь, после чего на следующий день вновь отпустят.

После того как СЕМЕНИК прошёл процедуру по делу о побеге и был выпущен, мы забрали его. ФБР согласилось выделить средства на размещение СЕМЕНИКа в гостинице, обеспечение суточными и транспорт домой. СЕМЕНИКа поселили в апартаментах отеля Mission Valley Marriott. Ему было предоставлено право свободно распоряжаться своим временем и видеться с друзьями когда угодно.

В период пребывания СЕМЕНИКа в Marriott либо я, либо агент Мозес занимали соседний с его номером. За три дня в гостинице СЕМЕНИК сумел предоставить нам весьма полезные сведения и разведывательную информацию. Этого оказалось недостаточно для ареста, но кое-что ценное мы получили. Независимо верифицировать информацию из другого источника нам не удалось.

В период с 3 по 5 апреля 1992 года СЕМЕНИК по телефону связывался с многочисленными лицами, причастными к компьютерному хакерству. Он добровольно и без принуждения подписал форму согласия ФБР, разрешив нам записывать его телефонные разговоры в ходе расследования. Было записано множество телефонных переговоров с участием не менее 4 отдельных лиц.

В тот же период с компьютера некоего лица, находившегося на Восточном побережье, на наш компьютер в формате данных была скачана информация. Полученные в ходе загрузки материалы представляли собой актуальные кредитные отчёты, только что полученные этим лицом из компании CBI, руководство по CBI, написанное отчасти «Kludge» — хакером из Сан-Диего, — а также многочисленные файлы и документы, касающиеся незаконной деятельности, в частности «кардинга». «Кардинг» — термин хакерского сообщества, обозначающий незаконное или мошенническое использование кредитных карт или их номеров хакерами по всей стране.

СЕМЕНИК сообщил, что в период своей активной хакерской деятельности состоял в местной BBS под названием Scantronics. По его словам, доску держит некий «KLUDGE», и на ней хранятся сотни файлов и документов. Большинство этих материалов, по его утверждению, являются инструкциями: они рассказывают тем, кто скачивает их через BBS Scantronics, как делать те или иные вещи — как законные, так и незаконные. В числе незаконных видов деятельности, освещённых на этой BBS, — кардинг, телефонное хакерство, мошенничество с банкоматами и информация о кредитных бюро.

Мы получили три документа, написанных или распространённых «KLUDGE» или BBS Scantronics.

ДАННОЕ РАССЛЕДОВАНИЕ В НАСТОЯЩЕЕ ВРЕМЯ ПРОДОЛЖАЕТСЯ; ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ И ДОКАЗАТЕЛЬСТВА БУДУТ ДОБАВЛЕНЫ.

Полицейское управление Сан-Диего — Дополнительный рапорт следователя

```
НОМЕР ДЕЛА: N/A
ДАТА:       30 апреля 1992 года
ВРЕМЯ:      07:00
ТЕМА:       Компьютерное хакерство
ПОДОЗРЕВАЕМЫЙ: N/A
ПОТЕРПЕВШИЙ:   N/A
МЕСТО:      N/A
ДЕТЕКТИВ:   Dennis W. Sadler (уд. № 2486)
```

16 апреля 1992 года со мной связался Кевин Маркус. Маркус узнал, что мы ведём расследование в отношении лиц, незаконно входящих (взламывающих) в различные компьютерные системы по всей стране. Маркус управляет местной компьютерной доской объявлений (BBS) под названием The Programmer's Paradise. Его беспокоила незаконная деятельность, которую он наблюдал на различных местных BBS, — он и обратился ко мне.

Маркус также сообщил, что получил компьютерные сообщения от человека с ником Knight Lightning из Нью-Йорка, который спрашивал, слышал ли он что-нибудь о нашем расследовании. Knight Lightning рассказал Маркусу, что 3 апреля репортёр из Сан-Диего по имени Бигело связался с ним и расспрашивал о нашем текущем расследовании.

Приложение 1:

```
Date: Fri, 10 Apr 1992 18:14:11 -500
To: knight@eff.org
From: Craig Neidorf <knight@eff.org>
Subject: Runaway Teen Hacker Picked Up?

Только что со мной связался репортёр из Сан-Диего по поводу хакерского дела.

По всей видимости, некий юный хакер из Индианы сбежал из дома
в Калифорнию — навестить какую-то девушку. Местная полиция и ФБР
якобы задержали его 3 апреля, и он по сей день находится у них
без предъявления обвинений, рассказывая всяческую информацию
о хакерских кольцах по всей стране.

Есть ли у кого-нибудь зацепки относительно того, кто этот парень
и что происходит?

:Knight Lightning
```

Приложение 2:

```
Date: Thu, 16 Apr 1992 22:25:17 -0400
From: Craig Neidorf <knight@eff.org>
To: tck@netlink.cts.com
Subject: Re: Hi.

Брюс Бигело, Union Tribune. Оставил номер в офисе. Ничего нового,
но понимаю, что ты ему звонил.

Craig
```

Маркус предложил помочь. Я спросил, знает ли он BBS под названием Scantronics. Он ответил утвердительно: был её участником и в прошлом просматривал файлы на этой доске, чтобы понять, что там есть. Маркус учится на факультете компьютерных наук в местном колледже и занимается исследованиями в области антивирусной защиты. По его словам, на доске имелось много технических данных, но ничего по его теме. Маркус также состоит в других местных и иногородних BBS, где общается с людьми, разделяющими его интересы.

Маркус рассказал, что примерно месяц назад последний раз заходил на BBS Scantronics и видел там многочисленные компьютерные файлы, касающиеся CBI и кардинга. Кардинг — термин, используемый хакерами, занимающимися незаконным или мошенническим использованием кредитных карт и их номеров. Номера кредитных карт получают из компаний, предоставляющих кредитные отчёты, — таких как CBI и TRW, — путём незаконного взлома их компьютеров и считывания или копирования частных кредитных отчётов и персональных данных граждан.

Большинство кредитных отчётов этих компаний содержат имя человека, текущий и предыдущие адреса, номер социального страхования, место работы, зарплату и всю актуальную кредитную историю, включая все кредитные карты с их номерами счетов. Полученные номера хакеры используют для приобретения товаров.

Если кто-то из хакеров воспользовался номером счёта из незаконно скачанного кредитного отчёта, жертва, скорее всего, обнаружит незаконное списание не раньше следующего биллингового цикла — то есть спустя до 45 дней после совершения мошеннической операции. По данным индустрии кредитных карт, это один из наиболее безрисковых способов совершения карточного мошенничества.

Маркус сообщил, что человека, ведущего эту BBS, зовут Джереми. Фамилию он не знал, но известен тот под ником «KLUDGE». На вопрос о телефонном номере BBS Маркус назвал 423-4852. Номер телефона, имя оператора и его ник совпали с информацией, полученной нами ранее.

Маркус также передал мне два диска с файлами, скачанными (оставленными) на его BBS другими пользователями системы. Он регулярно проверяет свою доску и удаляет файлы, касающиеся сомнительной или незаконной деятельности, в частности кардинга.

Я просмотрел оба диска — они содержали весьма интересные файлы: руководство по угону автомобилей, руководство по CBI, руководство по TRW, информацию о картах American Express и многие другие файлы, которые при скачивании или копировании давали бы любому желающему возможность незаконно получить доступ к различным бюро кредитных историй и совершать иные виды незаконной деятельности.

Я попросил Маркуса сообщать мне, если он столкнётся с дальнейшей информацией подобного рода или о BBS Scantronics.

17 апреля 1992 года я встретился с Маркусом. Он рассказал, что накануне ночью заходил на Scantronics, воспользовавшись номером доступа, который ему дал приятель. Этот же приятель неоднократно позволял ему использовать свой аккаунт для входа на эту BBS прежде. Маркус сделал это по собственной инициативе, без каких-либо указаний с моей стороны или со стороны других сотрудников правоохранительных органов.

Маркус передал мне компьютерный диск формата 5,25 дюйма и сообщил, что на нём содержится список файлов и перечень всех подтверждённых пользователей. Маркус также сообщил, что на диске есть копия сообщений, которые человек из Нью-Йорка отправил ему через его BBS в связи с нашим расследованием (приведённые выше сообщения от Knight Lightning).

Он спросил, хочу ли я, чтобы он вошёл на BBS «KLUDGE'a» и показал мне её содержимое лично. Я ответил, что сначала должен проконсультироваться с прокуратурой. Однако связаться с нашим куратором из прокуратуры мне не удалось. Я пообещал Маркусу вернуться к этому позже.

Поговорив с помощником прокурора Майком Карлтоном, я посоветовал Маркусу не заходить на BBS Scantronics, если только это не в его личных интересах. Однако он сказал, что если в ходе обычной работы со своей BBS он наткнётся на какую-либо дополнительную информацию — уведомит меня.

[Полицейский рапорт также содержал 60 страниц распечаток публикаций и текстовых файлов, обнаруженных на BBS Scantronics. Особо подчёркивается, что Кевин Маркус (известный как The Crypt Keeper) входил на BBS Scantronics, используя пароль и номер аккаунта The Gatsby. В числе файлов:

• «Credit Bureau Information» («Информация о кредитных бюро») — звучит безобидно, однако оказывается перепечаткой статьи из номера журнала Business Week от 27 сентября 1992 года.
• «Advanced Carding» («Продвинутый кардинг») — авторство The Disk Jockey, датируется 1987 годом.
• «The Complete CBI Manual of Operations» («Полное руководство по операциям CBI») — авторы Video Vindicator и Kludge, датировано 10 октября 1991 года.]

Последствия

23 апреля 1992 года в муниципальном суде штата Калифорния округа Сан-Диего был выдан ордер на обыск, санкционировавший изъятие:

A. Всей абонентской информации телефонной компании, включая дату начала обслуживания, копию последнего счёта, актуальную кредитную информацию и место подключения телефонной линии по следующим номерам: (619)XXX-XXXX и (619)XXX-XXXX, а также любую иную информацию по номерам в любой цепочке переадресации звонков, идущих на указанные или с указанных номеров.

B. Всей документации телефонной компании, включая абонентскую информацию, дату начала обслуживания, копию последнего счёта, актуальную кредитную информацию и место подключения для номеров, на которые переадресовываются или с которых переадресовываются звонки от указанных номеров.

```
                УДОСТОВЕРЕНИЕ ОБ ОТСРОЧКЕ УВЕДОМЛЕНИЯ АБОНЕНТА

    Суд установил наличие существенных вероятных оснований полагать,
    что уведомление абонента, чья деятельность зафиксирована в
    описанных выше записях, воспрепятствует или уничтожит данное
    расследование. Соответственно, суд удостоверяет ходатайство
    Полицейского управления Сан-Диего об отсрочке уведомления
    абонента до особого распоряжения суда.
```

30 апреля 1992 года в муниципальном суде штата Калифорния округа Сан-Диего был выдан ордер на обыск по месту жительства Kludge и изъятие:

> *Всего компьютерного оборудования и сопутствующих предметов, используемых при компьютерном хакерстве или являющихся частью BBS Scantronics, включая (без*

ограничения): мониторы, клавиатуры, системные блоки (которые могут содержать жёсткие диски, дисководы для дискет, накопители на магнитной ленте, приводы CD-ROM), модемы, факс-модемы, все бумажные копии любых компьютерных файлов, хранившихся или хранящихся в компьютерной системе, все документы в твёрдой или цифровой форме, содержащие инструкции по работе с любой компьютерной программой или файлом, все устройства хранения данных, включая жёсткие диски, дискеты 5,25 и 3,5 дюйма, резервные ленты и диски CD-ROM, способные хранить компьютерные данные; а также документы и предметы, подтверждающие господство и контроль над указанными помещениями и компьютерной системой, в том числе отпечатки пальцев, записи, рукописи, документы и предметы с идентификационными данными — именем лица, фотографией, номером социального страхования или водительского удостоверения, а также ключи.

Ордер был немедленно исполнен — BBS Scantronics и многое другое было изъято.

The Crypt Keeper отвечает

```
Date: Wed, 17 Jun 92 09:13:50 PDT
From: tck@bend.UCSD.EDU (Kevin Marcus)
To: knight@eff.org
Subject: Hmm.
```

Начну с самого начала...

3 апреля, около 15:00, я пришёл на своё рабочее место (компьютерный магазин). Multiplexor сидит в подсобке с каким-то агентом ФБР и детективом Деннисом Садлером. Причина, по которой они выбрали именно наш магазин для технической поддержки, — Деннис очень хорошо знаком с одним из моих менеджеров.

Я видел, что происходит, и видел, как Multiplexor пытается зайти на доску Kludge'a — но его не подтвердили. Тем не менее в тот же день я предупредил Gatsby и Kludge о том, что происходит, поскольку они были моими друзьями и я не хотел, чтобы с ними случилось что-то плохое.

Через несколько дней мой босс посоветовал мне сказать Деннису, что я бывал на доске Kludge'a когда-то давно, но теперь туда не хожу — мол, они могли что-то на меня найти. Поэтому при следующей встрече (Деннис заходит примерно раз в неделю, до сих пор) я сказал ему, что бывал на доске, но давно. Он задал несколько глупых вопросов, я особо ничего не сказал.

В итоге он каким-то образом узнал, что я предупреждал Kludge о его доске. Как — я понятия не имею, сам я ему этого точно не говорил. Тогда Деннис сказал мне, что я едва не сорвал их расследование, а за вмешательство в расследование максимальный срок — что-то вроде 5 лет. Он уже собирался меня арестовать и отвезти в окружной суд, когда моему боссу удалось убедить его, что я нормальный парень, не ищущий неприятностей, и что я принесу ему что-нибудь, чтобы укрепить его позицию. Так что, хотя Деннис и не говорил мне прямо что-то добыть с доски Kludge'a, он дал понять, что для восстановления дела ему нужно представление о том, что там есть, — что-то вроде буферной копии системы.

В ту ночь я позвонил Gatsby и получил от него пароль. Зашёл и сделал буферную копию. При следующей встрече с Садлером я рассказал ему, что сделал. Он хотел знать, как я попал на доску Kludge'a, и я сказал — через аккаунт приятеля. Спросил, чьего. Я ответил: «The Gatsby». Тогда он начал задавать вопросы о Gatsby: «Как его настоящее имя?» Сначала я сказал, что не хочу говорить, но он заявил, что я скрываю улики и может арестовать меня уже за это. Тогда я назвал его имя и сообщил, что тот живёт в XXXXX (пригород Сан-Диего). Они и без того уже записывали

Gatsby и Kludge в телефонных разговорах по линии Kludge'a, которая прослушивалась какое-то время, так что кто он такой — они уже знали.

Если бы над моей головой не висели такие вещи, как вмешательство в расследование и сокрытие улик, я бы, скорее всего, вообще рта не раскрыл. Моим первым контактом с ним стал совет моего босса, который близко с ним знаком, и, возможно, тот сказал боссу что-то такое, что заставило его беспокоиться и думать, что меня могут арестовать. Точно не знаю.

Если бы я был стукачом — уверяю вас, много больше людей оказалось бы за решёткой. У меня масса информации о том, кто есть кто, кто где находится, кто чем занимается, — и, хоть она и устаревшая, держу пари, многое из неё по-прежнему верно. Если бы я хотел устроить ещё одну Операцию Солнечный Дьявол — я бы отдал ему всё это. Но не отдал, потому что это не входило в мои намерения. Я не хотел, чтобы кто-либо попался (включая меня самого) ни за что.

Если бы я был стукачом — разве я не дал бы ему куда больше информации?

Я так думаю.

Я не прошу никого забыть об этом. Я понимаю, что напортачил, и мало что могу сейчас исправить.

Когда Садлер задавал мне вопросы, мне не пришло в голову сказать ему подождать, позвонить адвокату, а потом вернуться и сказать всё, что посоветует адвокат. Я был напуган.

Хакеры — не настоящий враг — 8 июня 1992 года

Автор: Chris Goggans (ComputerWorld, стр. 37)

(Гоггансу 23 года, он хакер, в настоящее время ищет работу у того, кто не заставит его стричь волосы.)

На протяжении многих лет выходили статьи о людях, называющих себя «хакерами». Их писали те, кто расследовал деятельность хакеров, кто становился их мишенью, кто защищает системы от хакеров и кто утверждает, что лично их знает. Как член так называемого «компьютерного андеграунда», я хотел бы представить точку зрения самих хакеров.

Надеюсь, вы отложите в сторону личные предубеждения в отношении людей, называющих себя хакерами, — ведь они, скорее всего, основаны не на реальном знакомстве с ними, а на материалах в СМИ.

Надеюсь также, что вы не откажетесь читать этот текст из-за разногласий с моей этикой. За последние 11 лет, действуя под псевдонимом Erik Bloodaxe, у меня были возможности несказанно разбогатеть и нанести чудовищный ущерб мировым компьютерным сетям. Однако я не сделал ни того ни другого. Я заглядывал за двери с табличками «Только для персонала», но никогда не нарушал работу бизнеса. Вуайеризм — это совсем не то же самое, что насилие.

Незаконное, но не уголовное

Бесспорно, действия некоторых хакеров незаконны, однако по своему характеру они едва ли являются уголовными. Намерение большинства этих людей — не разрушать системы и не эксплуатировать их, а лишь досконально изучить, как они устроены и для чего используются. Поиск носит сугубо интеллектуальный характер, однако жажда знаний столь велика, что любое препятствие на её пути будет обойдено. К сожалению, препятствиями чаще всего служат государственные и федеральные законы о несанкционированном доступе к компьютерам.

Принципиальное отличие сегодняшних хакеров от их тёзок из MIT 1960-х годов состоит в том, что многие мои современники начали свою деятельность в слишком юном возрасте, чтобы иметь свободный доступ к компьютерным системам. Редкий тринадцатилетний подросток получает привилегии системного пользователя на VAX обычным путём.

Моим первым компьютером был 8-битный Atari с 16 килобайтами памяти. Я быстро понял, что возможности такой машины крайне ограничены. Однако с приобретением модема передо мной открылся целый мир: внезапно в моём распоряжении оказалась вычислительная мощь на самом современном уровне — на удалённых узлах по всему миру. Нередко доступ мне давали просто в ходе разговора с администраторами об уязвимостях в их системах, но чаще единственным доступом был тот аккаунт, на который я случайно натыкался.

Многие с трудом понимают, зачем кто-то будет рисковать уголовным преследованием ради изучения компьютерной системы. Я сам задавал себе этот вопрос неоднократно и не нахожу однозначного ответа. Знаю лишь, что это зависимость — настолько сильная, что, если не уравновешивать её другими занятиями, она может перерасти в тотальную одержимость. Каждый хакер из тех, кого я знаю, проводил дни без сна, прочёсывая закоулки компьютерных сетей, тестируя утилиты и читая файлы. Мне самому случалось так погружаться в проект, что я забывал поесть.

Хакеры почти не имеют общих демографических черт: они принадлежат к самым разным социальным слоям, расам, вероисповеданиям и происходят из самых разных стран. Тем не менее некоторые общие черты всё же есть. Одна из них — обсессивно-компульсивное поведение (злоупотребление наркотиками или алкоголем, азартные игры, мелкие кражи). Для других характерна история разводов в семье, высокий интеллект (от одарённого до гениального уровня), плохие учебные навыки и недоверие к любым авторитетам. Большинству хакеров также свойственны природная паранойя и тяга к романтике — что хорошо заметно по ярким псевдонимам, распространённым в хакерском сообществе.

Однако в большинстве случаев, достигая студенческого возраста или возраста трудоустройства, хакеры получают более свободный доступ к интересующим их системам законными путями, и необходимость нарушать закон ради обучения отпадает.

Массовые медиа во многом поспособствовали негативному употреблению слова «хакер». Любой человек, уличённый в злоупотреблении картой для звонков на дальние расстояния или иной кредитной картой, именуется хакером. Любой, кто взломал систему безопасности компьютера, также называется хакером и преподносится как компьютерный гений — хотя даже человек с самой базовой компьютерной грамотностью способен взломать компьютерную защиту, если постарается.

Вопреки тому, что внушают СМИ, всё статистика говорит, что хакеры никогда не были более чем каплей в море в части серьёзных компьютерных преступлений. В действительности хакеры редко бывают чем-то большим, чем временным неудобством, — если их вообще замечают. Настоящая опасность состоит в том, что их методы легко воспроизводятся людьми с куда более зловещими мотивами. Текстовые файлы и прочая информация, которую хакеры публикуют в компьютерных системах, могут быть использованы потенциальным корпоративным шпионом для выработки плана атаки на компанию.

Учитывая, что о существовании и возможностях хакеров осведомлены практически все — а также о том, как другие могут пройти через двери, открытые хакерами, — полное отсутствие безопасности в мировых компьютерах просто поражает.

Точки входа

Главная проблема — плохое системное администрирование. Пользователям разрешено выбирать легко угадываемые пароли. Права доступа к директориям заданы неправильно. Надлежащий учёт процессов игнорируется. Утилиты для решения этих проблем существуют для каждой операционной системы, однако широкого применения они не нашли.

Многие системные администраторы лишены доступа к актуальной информации, необходимой для защиты их систем. Между вендорами и заказчиками, а также внутри корпоративного сообщества в целом царит ужасающий информационный вакуум.

Вместо того чтобы сообщать всем об уязвимостях по мере их обнаружения, вендоры хранят информацию в секретных базах данных безопасности или передают её избранным через списки рассылки по электронной почте. Это почти не помогает исправить ситуацию — более того, лишь усугубляет её, поскольку многие хакеры имеют доступ к этим базам данных и архивам информации из таких рассылок.

Ещё одна серьёзная проблема в системной безопасности связана с телекоммуникационным оборудованием. Различные телефонные компании Bell давно стали мишенями хакеров, и многие из них знают, как управлять корпоративными и центральными офисными системами, лучше, чем техники, работающие с ними за зарплату.

Всё более широкое использование компьютерных сетей добавило принципиально новое измерение незащищённости. Если компьютеру разрешено общаться с другим в рамках одной сети, каждый компьютер в цепочке должен быть неприступен — иначе под угрозой оказывается безопасность всех узлов. Наиболее яркие примеры этого — ситуации в Интернете. При таком разнообразии проблем и столь скудном количестве доступной информации об их решении сфера консалтинга в области компьютерной безопасности стремительно растёт. К сожалению, то, что компании покупают, — это иллюзия безопасности. Главные игроки здесь — крупные аудиторские фирмы. Однако их дорогостоящие аудиты носят преимущественно процедурный характер и редко проводятся специалистами с достаточным уровнем технической экспертизы, чтобы их рекомендации имели реальный и долгосрочный эффект.

В конечном счёте обязанность обеспечить себя нужными инструментами для защиты своих систем от вторжения лежит на системных администраторах. Получить необходимую информацию бывает непросто, однако если посторонние могут до неё добраться — значит, смогут и те, кому платят за эту работу.

Великий спор

Киберпанк встречает Мистера Безопасность — июнь 1992 года

Автор: Jonathan Littman (PC Computing Magazine, стр. 288)

Phiber Optik против Donn Parker

Юноша осторожно подошёл к столику и спросил высокого, представительного лысого джентльмена в сером костюме, не против ли тот, если он присоединится. На бейдже юноши значилось «Phiber Optik», на бейдже джентльмена — «Donn Parker». Один был членом Legion of Doom — печально известной группы молодых хакеров, которым в 1990 году предъявили обвинения в мошенничестве, сговоре и незаконном доступе к компьютерам; другой — легендарным экспертом по безопасности.

Эту маловероятную пару свёл необычный форум — первая в истории страны конференция «Компьютеры, свобода и приватность», прошедшая в районе залива Сан-Франциско в последние выходные марта 1991 года. Они были частью пёстрой аудитории из агентов ФБР, сотрудников Секретной службы, прокуроров, защитников приватности и хакеров, собравшихся вблизи посмотреть друг на друга.

Лишь несколькими неделями ранее ноутбук Optik'a был изъят полицией штата в ходе расследования, начатого Секретной службой. Optik и его товарищи-хакеры Acid Phreak и Scorpion оказались среди первых, попавших в поле зрения Секретной службы в дни Операции «Солнечный Дьявол» — облавы в 14 городах весной 1990 года, в ходе которой было изъято 42 компьютера, 23 000 дискет и произведено четыре ареста.

Уголовные обвинения, предъявленные Optik'у и его сообщникам, включали незаконный доступ к компьютерам и торговлю похищенными кодами доступа. Optik, бывший несовершеннолетним на момент первоначального допроса, провёл день под стражей и впоследствии был осуждён за мисдиминор — кражу услуг.

Паркер хорошо знал эту историю. На протяжении последних двух десятилетий бывший учитель воскресной лютеранской школы провёл интервью с десятками преступников, для которых компьютеры были лишь инструментом ремесла. Попутно он снискал мировую репутацию «белоголового орлана» компьютерных преступлений. Паркер часто выступает перед правоохранительными органами и корпорациями как консультант SRI International — ведущей исследовательской и управленческой компании в Менло-Парк, Калифорния. Его книги «Fighting Computer Crime» и «Crime by Computer», многочисленные статьи и объёмное исследование по компьютерной этике для Министерства юстиции закрепили за ним статус главного авторитета в изучении психологии хакеров.

ПАРКЕР: Как вы оцениваете этику проникновения в чужие компьютерные системы?

OPTIK: Я знаю вашу точку зрения — читал ваши работы, слушал ваши выступления. Знаю, что вы считаете любое вторжение, любой несанкционированный доступ уголовным преступлением.

Не могу сказать, что согласен с этим. Согласен, что любой впечатлительный подросток, который встрял в это и хочет взломать как можно больше компьютеров, чтобы что-то доказать, потенциально способен причинить ущерб — потому что он несовершеннолетний, понятия не имеет, что делает, и лезет туда, куда ему нет дела.

В то время мне было 17 лет, я был несовершеннолетним. У меня не было никакой возможности купить Unix, VAX, собственную коммутационную систему. Именно этому я хотел научиться программировать. Получить доступ к такой вычислительной среде разработки без умения взламывать системы было бы невозможно. Я смотрю на это именно так.

ПАРКЕР: Что вы делаете на этой конференции? Какова ваша цель?

OPTIK: В основном я хочу встретиться с как можно большим числом людей и выслушать как можно больше точек зрения.

ПАРКЕР: В чём ваша конечная цель — чего вы хотите добиться с точки зрения карьеры? Считаете ли вы, что это путь к карьере?

OPTIK: Разумеется, я надеюсь войти в компьютерную индустрию. Хотя бы тем, что я здесь, я надеюсь поговорить с такими людьми, как вы, со многими профессионалами в этой области, услышать их взгляды и поделиться своими.

Видите ли, больше всего меня огорчает то, что существует разрыв в коммуникации, отсутствие диалога между теми, кто называет себя хакерами, и компьютерными профессионалами. Думаю,

если бы между более респектабельными хакерами и компьютерными профессионалами существовал лучший диалог, он был бы куда продуктивнее.

ПАРКЕР: Как отличить хакера более ответственного типа?

OPTIK: Понимаю, что это очень серьёзная проблема. Вижу, что это практически невозможно — и прекрасно понимаю, как вы приходите к выводам, которые формулируете в своей статье: что хакеры известны обманом, ложью и преувеличениями. Я сталкивался с этим постоянно — своими глазами. В общем-то, эти люди именно таковы. Просто помните, что значительная часть из них — вовсе не закоренелые хакеры: это впечатлительные подростки, тусующиеся в Сети. Просто среда, в которой они тусуются, — это компьютеры.

Я совершенно не считаю себя частью этой компании. Я пришёл к компьютерам рано — ещё в начальке. Я был совсем юным — лет двенадцать-тринадцать, когда мне на Рождество подарили компьютер.

В Сеть я сразу не полез. Я не из тех нынешних детей, которым дарят Commodore 64 с модемом на Рождество за хорошие оценки. Я называл себя хакером потому, что хакил в смысле исследования мира внутри своего компьютера — языки ассемблера, машинные коды, электроника, и всё такое прочее. Вот что меня по-настоящему интересовало.

Вся эта социальная онлайн-история — без неё я вполне мог бы обойтись, потому что именно оттуда и берутся эти идеи. Знаете, весь этот негатив, это горькое послевкусие, которое остаётся, когда слышишь, как кто-то поливает грязью хакерскую сцену целиком. Это потому, что люди слышат определённые вещи, а слышат они их от наиболее крикливых персонажей этого «компьютерного андеграунда» и из искажённых публикаций в СМИ, которые гонятся за сенсацией.

И расплачиваются за это такие люди, как я. А профессионалы получают искажённую картину — потому что слышат только самых громких. Ещё одна причина, по которой я здесь: я хочу, чтобы люди знали, что существуют и уважаемые хакеры. Хакерство — это больше, чем впечатлительные малолетние хулиганы.

ПАРКЕР: Как бы вы определили хакерство?

OPTIK: Это общее желание понять технологии, уметь общаться с машиной на очень низком уровне, уметь её программировать. Когда я вижу компьютер, мой мозг хочет поговорить с его микропроцессором. Вот моя философия в двух словах.

ПАРКЕР: Важно ли вам, кто на самом деле является владельцем компьютера?

OPTIK: Как правило, важно. О, поначалу — не важно. Сам факт проникновения в Unix и освоения Unix был достаточно важен, чтобы оправдать моё присутствие в системе. Не из-за информации, которая там хранится. Меня на самом деле не интересует, что это за информация.

Знаете, есть такое целое киберпанк-направление, которое считает, что информация должна быть свободной. Я же целиком верю в компьютерную приватность. Если кто-то хочет, чтобы что-то было приватным, — пусть будет. Информация не предназначена для всеобщего доступа, если вы изначально проектируете её как приватную. Именно для этого и существует такая вещь, как безопасность.

Если кто-то хочет держать что-то в тайне, я не стану пытаться это прочитать. Меня это не интересует. Мне всё равно, что люди пишут друг другу по электронной почте. Я там потому, что меня интересует железо.

ПАРКЕР: Откуда кому-то знать, что вы не заинтересованы в чтении их личной почты?

OPTIK: Это моя проблема, с которой мне придётся разбираться. Реального решения здесь нет — точно так же, как нет надёжного способа определить, злонамерен ли человек. Хакеры действительно хвастаются, обманывают и преувеличивают. Могут сказать вам одно, а потом

ударить в спину и сказать совсем другое.

ПАРКЕР: Я провёл интервью более чем со 120 так называемыми компьютерными преступниками.

OPTIK: Да.

ПАРКЕР: Я интервьюировал многих хакеров, а также многих людей, вовлечённых в самые разные виды беловоротничковой преступности.

OPTIK: Угу.

ПАРКЕР: И мне кажется, что люди, с которыми я разговаривал, осуждённые за злонамеренное хакерство и сумевшие преодолеть и перерасти всё это, пошли на законные должности в системном программировании — там, где есть серьёзный вызов, и они очень успешны. Они больше не занимаются злонамеренным хакерством или преступной деятельностью и строят карьеру в технологиях, которые любят.

OPTIK: Верно.

ПАРКЕР: Почему вы не могли пойти по этому пути? Почему не получить квалификацию, отучившись в школе, как я и как все, кто работает профессионалом в компьютерной сфере, и найти интересную работу в компьютерных технологиях?

OPTIK: Я очень надеюсь получить интересную работу в компьютерных технологиях. Но я просто чувствую, что там, где я живу, школьная система, в которой я нахожусь, не отвечает моим потребностям в стремлении как можно больше узнать о технологиях как можно быстрее.

ПАРКЕР: Да, но одно из того, чему нужно научиться, — это терпение, и нужно быть готовым работать усердно и осваивать технологии в том темпе, как они преподаются.

OPTIK: Знаете, просто помните, что благодаря возможности бывать там, куда людям нельзя, я узнаю о технологиях то, чего школы не преподают. Просто программы в местных колледжах, где я живу, даже близко не могут охватить того, что я пережил.

ПАРКЕР: Значит, вы хотите мгновенного результата.

OPTIK: Дело не столько в результате...

ПАРКЕР: Вы не готовы провести четыре года в...

OPTIK: Я определённо готов учиться в университете.

ПАРКЕР: Хорошо.

OPTIK: Я твёрдо намерен поступить в университет; просто не жду, что узнаю там очень многое о технологиях. Жду, что узнаю кое-что о технологиях, о чём, вероятно, не знаю, но не рассчитываю соприкоснуться с таким же разнообразием технологий, как в мои подростковые годы.

ПАРКЕР: Понимаю нетерпение и нехватку возможностей сделать всё это быстро, но...

OPTIK: Я бы не назвал это нетерпением. Я бы назвал это жаждой учиться.

ПАРКЕР: Жажду учиться можно применять в рамках установленного образовательного процесса самыми разными способами. В школе можно достигать выдающихся результатов.

OPTIK: Я никогда не был заядлым отличником, скажу прямо. Школа меня в основном не интересует. Обычно я компенсирую это чтением технических руководств.

ПАРКЕР: Как вы проведёте четыре года в школе, если уже решили, что вам там неуютно?

OPTIK: Ну, дело не столько в школе, сколько в том, что я чувствую себя стеснённым в средней школе и через то, что мне приходится проходить через восемь и девять классов из-за того, как выстроена образовательная программа...

ПАРКЕР: Что ж, если вы будете придерживаться нынешнего пути, вы вполне можете оказаться техником, ремонтирующим оборудование, обслуживающим компьютеры — и вполне можете зайти в тупик.

Чтобы выйти на более высокий уровень работы, нужен билет — диплом, нужно доказать, что вы умеете учиться и получать приемлемые оценки. Путь, который вы избрали, мне не кажется ведущим к этому.

Есть, конечно, люди, которым удалось это преодолеть — Джефф Гудфеллоу, Стив Возняк. Но такие — один на сто тысяч. Все остальные девяносто девять тысяч — техники. Они живут нормально, зарабатывают нормально, но ничего великого не совершают. Просто поддерживают оборудование в рабочем состоянии.

OPTIK: Да.

ПАРКЕР: И если у вас есть всё это любопытство, этот драйв, эта энергия — то, что для этого нужно, — и вы идёте путём, который приведёт вас туда, где можно заниматься настоящими, захватывающими, передовыми исследованиями... Я знаком со многими хакерами. Думаю об одном из Вашингтона, осуждённом за компьютерное преступление. Он вернулся учиться, получил диплом и занимает очень высокую должность в системном программировании. Он сказал, что в какой-то момент решил: нужно менять подход, потому что при сложившемся ходе вещей его будущее выглядело весьма мрачно.

И мне кажется, что, возможно, вы со временем придёте к осознанию: чтобы делать важные, захватывающие вещи, в конечном счёте нужно освоить научный путь в компьютерах — понять, как устроены операционные системы, как писать программы очень большого и сложного характера.

Вы когда-нибудь этим занимались — писали по-настоящему большую компьютерную программу?

OPTIK: Я написал это...

ПАРКЕР: Здесь нужна дисциплина, которая связана с обучением инженерному мышлению. Это требует колоссального образования и самодисциплины. И мне кажется, что вам не хватает дисциплины. Вы хотите мгновенного результата, хотите быть экспертом прямо сейчас. И вы действительно становитесь экспертом — но в очень узкой области технологий.

Вы изучаете сеть Novell LAN, осваиваете какой-то другой аспект, узнаёте о коммутационных системах телефонной компании. Всё это не ведёт к карьере в области проектирования и разработки систем. Это ведёт к карьере в обслуживании того железа, которое вы взламываете.

И мне кажется, что нужно вернуться и изучить принципы. Каковы базовые принципы операционной системы? Каковы базовые принципы управления доступом? Пока вы не вернулись и не изучили эти основы, вы летите на ощупь, подбирая обрывки всего того, что можно быстро схватить.

OPTIK: Я не считаю, что хватаю вещи быстро. Я потратил много времени на изучение очень детальных вещей. Это не «вскочил — выскочил, и рад чему попало». Я действительно провожу много времени за руководствами и прочим.

ПАРКЕР: Руководства вас не спасут. Изучая руководство, вы узнаёте только нынешнее оборудование и принцип его работы. Если бы вы изучили тома Дональда Кнута по компьютерному программированию и компьютерным наукам, вы бы усвоили теорию компьютерного программирования, теорию операционных систем — теорию, которая является фундаментом всех этих систем.

OPTIK: Но вот в чём дело — наверное, этим я и не занимаюсь. Меня никогда особо не занимала теория работы. Меня всегда интересовало, как всё устроено и как я могу этим пользоваться. Как программировать. Признаю, что теория меня никогда не увлекала. Она мне не интересна. В том, чем я занимаюсь, теория сейчас никакой роли не играет. Впрочем, это может измениться в любой

момент. Я ещё достаточно молод...

Приятель шепнул Optik'у на ухо, что пора идти. Всё ещё в разгаре спора, хакер и специалист по безопасности встали из-за стола и вместе направились к эскалатору. В профиль, у подножия движущейся лестницы, они выглядели странной парой: Optik с блестящими иссиня-чёрными волосами — и Паркер с блестящим куполом черепа.

Паркер спокойно говорил, предупреждая Optik'а, что однажды хакерство покажется не таким безграничным, а возможностей останется куда меньше. Optik беспокойно ёрзал, отводя взгляд. Участники конференции один за другим поднимались на эскалаторе.

— Я не хочу быть хакером вечно, — вдруг выпалил Optik.

На следующий день после полудня у рядка гостиничных телефонов толпились деловые люди и участники конференции — звонили, слушали сообщения. Среди них был и Optik: зажатый между костюмами, с акустическим соединителем на телефонной трубке, перед мерцающим экраном ноутбука, пальцы порхают по клавишам.

Он всё ещё был молод.

MOD предъявлены обвинения

8 июля 1992 г.

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                               PWN
PWN               Phrack World News               PWN
PWN                                               PWN
PWN            Issue 40 / Part 2 of 3             PWN
PWN                                               PWN
PWN         Compiled by Datastream Cowboy         PWN
PWN                                               PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Datastream Cowboy

Источник: U.S. Newswire

Ниже приводится пресс-релиз, выпущенный Офисом прокурора США по Южному округу Нью-Йорка.

Группа «компьютерных хакеров» обвинена в суде
Первое применение прослушивания телефонных переговоров в подобном деле

НЬЮ-ЙОРК — Группа из пяти «компьютерных хакеров» обвинена большим федеральным жюри Манхэттена в компьютерном взломе, компьютерном мошенничестве, мошенничестве с использованием средств связи, незаконном прослушивании и сговоре. Это стало первым случаем применения санкционированного судом прослушивания в ходе расследования с целью перехвата переговоров и передачи данных компьютерных хакеров.

Компьютерный хакер — это человек, использующий компьютер или телефон для несанкционированного доступа к другим компьютерам.

Согласно обвинительному заключению, поданному сегодня, Хулио Фернандес (псевд. «Outlaw»), Джон Ли (псевд. «Corrupt»), Марк Абене (псевд. «Phiber Optik»), Элиас Ладопулос (псевд. «Acid Phreak») и Пол Стайра (псевд. «Scorpion») проникли в широкий круг компьютерных систем, в том числе принадлежащих телефонным компаниям, кредитным бюро и учебным заведениям.

По словам Отто Г. Обермайера, прокурора США по Южному округу Нью-Йорка, Джеймса И. Хивея, специального агента, руководящего Нью-Йоркским отделением Секретной службы США, Уильяма И. Дорана, специального агента, руководящего уголовным отделом Нью-Йоркского отделения ФБР, и Скотта Чарни, начальника отдела по борьбе с компьютерными преступлениями Министерства юстиции, обвинительное заключение утверждает, что обвиняемые являлись членами тесно сплочённой группы хакеров, именовавшей себя «MOD» — аббревиатура, расшифровываемая по-разному: «Masters of Disaster» («Мастера катастрофы») или «Masters of Deception» («Мастера обмана»).

Согласно обвинительному заключению, обвиняемые взламывали компьютеры «для повышения своего образа и престижа в среде других компьютерных хакеров; для преследования и запугивания соперников-хакеров и других неугодных им людей; для получения телефонных, кредитных, информационных и прочих услуг без оплаты; а также для получения паролей, номеров счетов и иных ценных сведений, которые они могли бы продавать другим».

Кроме того, обвиняемые якобы использовали несанкционированные пароли и расчётные коды для бесплатных международных звонков и для доступа к другим компьютерам.

Среди компьютеров, в которые предположительно вторглись обвиняемые, — телефонные коммутационные компьютеры компаний Southwestern Bell, New York Telephone, Pacific Bell, U.S. West и Martin Marietta Electronics Information and Missile Group. Согласно обвинительному заключению, каждый из этих коммутационных компьютеров управляет телефонной связью десятков тысяч абонентских линий.

В ряде случаев обвиняемые предположительно вмешивались в работу компьютеров, добавляя и изменяя функции вызова. Некоторые местные номера были переадресованы на номера дальней связи, что позволяло получать услуги межгородских звонков по цене местных. По имеющимся данным, Southwestern Bell в 1991 году понесла убытки приблизительно в 370 000 долларов вследствие компьютерных вмешательств со стороны Фернандеса, Ли и Абене.

Обвинительное заключение также утверждает, что обвиняемые получили доступ к компьютерам BT North America — компании, эксплуатирующей сеть передачи данных Tymnet. Через доступ к компьютерам Tymnet они предположительно могли перехватывать передаваемые по сети данные, в том числе пароли сотрудников Tymnet. В одном из случаев Фернандес и Ли якобы перехватили передачу данных в сети Bank of America.

Также в числе обвинений — доступ к кредитным и информационным службам, включая TRW, Trans Union и Information America. Обвиняемые предположительно получали персональные данные граждан: кредитные отчёты, телефонные номера, адреса, сведения о соседях и номера социального страхования. В одном из случаев Ли и другой участник группы якобы обсуждали получение от другого хакера информации, позволяющей вносить изменения в кредитные досье TRW. Как следует из цитаты в обвинительном заключении, Ли сказал, что нужная ему информация позволит им «разрушить жизни людей... или сделать из них святых».

Далее обвинительное заключение утверждает, что в ноябре 1991 года Фернандес и Ли продали Мортону Розенфельду сведения о том, как получить доступ к кредитным службам. Позднее Фернандес якобы предоставил сообщникам Розенфельда номер счёта и пароль TRW, которые тот и его сообщники использовали для получения примерно 176 кредитных отчётов TRW на различных физических лиц. (В отдельном, но связанном судебном деле Розенфельд признал себя виновным в сговоре с целью использования и распространения номеров счетов TRW. См. ниже.)

Как сообщил помощник прокурора США Стивен Фишбейн, обвинительное заключение также утверждает, что члены MOD уничтожили почти всю информацию на компьютере Learning Link, принадлежащем Educational Broadcasting Corp. (телеканал WNET, канал 13) в Нью-Йорке. Компьютер Learning Link предоставлял образовательную информацию сотням школ и учителей в Нью-Йорке, Нью-Джерси и Коннектикуте. Конкретно: согласно обвинительному заключению, 28 ноября 1989 года информация на Learning Link была уничтожена, а на компьютере оставлено сообщение: «С праздником Благодарения, индейки, от всех нас из MOD», подписанное псевдонимами «Acid Phreak», «Phiber Optik» и «Scorpion». В ходе репортажа NBC News от 14 ноября 1990 года двое хакеров, скрывшихся за псевдонимами «Acid Phreak» и «Phiber Optik», взяли на себя ответственность за отправку этого сообщения.

Обермайер заявил, что предъявленные обвинения стали результатом совместного расследования Секретной службы США и ФБР. «Это первое федеральное расследование, когда-либо использовавшее санкционированное судом прослушивание для получения переговоров и передачи данных компьютерных хакеров», — сказал Обермайер, поблагодарив обе службы за обширную работу по данному делу и отметив важную помощь Отдела по борьбе с компьютерными преступлениями Министерства юстиции. Он также поблагодарил компании и учреждения, чьи компьютерные системы пострадали от действий обвиняемых: все они в полной мере содействовали расследованию.

Фернандес, 18 лет, проживает по адресу 3448 Steenwick Avenue, Бронкс, Нью-Йорк. Ли (также известный как Джон Фаррингтон), 21 год, — по адресу 64A Kosciusco Street, Бруклин. Абене, 20 лет,

— 94-42 Alstyne Avenue, Куинс. Элиас Ладопулос, 22 года, — 85-21 159th Street, Куинс. Пол Стайра, 22 года, — 114-90 227th Street, Куинс. Слушание дела назначено на 16 июля в 10:00 в федеральном суде Манхэттена.

Обвинения, изложенные в обвинительном заключении, являются лишь обвинениями; обвиняемые считаются невиновными до вынесения обвинительного приговора. Фишбейн сообщил, что в случае осуждения каждый из обвиняемых может быть приговорён к максимальному сроку пять лет заключения по статье о сговоре. Каждый из остальных пунктов обвинения также предусматривает максимум пять лет, за исключением обвинения Фернандеса во владении устройствами доступа, по которому грозит до десяти лет. Помимо этого, по каждому пункту предусмотрен максимальный штраф в размере 250 000 долларов или удвоенной суммы полученной прибыли либо нанесённого ущерба.

В отдельных, но связанных судебных делах было объявлено, что Розенфельд и Альфредо де ла Фе (псевд. Renegade Hacker) оба признали себя виновными в Федеральном окружном суде Манхэттена в сговоре с целью использования и распространения несанкционированных устройств доступа в связи с деятельностью, также затрагивавшей членов MOD.

Розенфельд признал вину 24 июня перед судьёй Федерального окружного суда Ширли Воль Крам. На слушании о признании вины Розенфельд признал, что покупал у хакеров номера счетов и пароли для TRW и других кредитных бюро, а затем использовал эту информацию для получения кредитных отчётов, номеров кредитных карт, номеров социального страхования и иных персональных данных, которые продавал частным сыщикам. Розенфельд также добавил, что около 25 ноября 1991 года он приобрёл у лиц по именам «Хулио» и «Джон» сведения о том, как несанкционированно получать доступ к кредитным службам. Он указал, что впоследствии он и его сообщники получили от «Хулио» дополнительные данные, которые использовали для многочисленных запросов кредитных отчётов. Согласно материалам дела, по которому Розенфельд признал вину, на 6 декабря 1991 года в его жилище находилось около 176 кредитных отчётов TRW.

Де ла Фе признал вину 19 июня перед судьёй Кеннетом Конбоем. На слушании де ла Фе признал, что использовал и продавал телефонные номера и коды для учрежденческих АТС (PBX). Согласно материалам дела, PBX — это частная автоматизированная телефонная система, маршрутизирующая звонки, обрабатывающая тарификацию и в ряде случаев позволяющая позвонившим получать исходящую связь по введённому коду. Де ла Фе признал, что продавал PBX-номера компании Bugle Boy Industries и других организаций сообщнику, который использовал их в схеме продажи звонков — то есть взимал с людей плату за международные переговоры по этим номерам. Де ла Фе также признал, что он и его сообщники пользовались PBX-номерами для бесплатных международных конференц-звонков; среди частых собеседников он назвал некоего Джона Фаррингтона, известного ему также под псевдонимом «Corrupt».

Розенфельд, 21 год, проживает по адресу 2161 Bedford Avenue, Бруклин. Альфредо де ла Фе, 18 лет, — 17 West 90th Street, Нью-Йорк. Оба обвиняемых освобождены до вынесения приговора под залог в 20 000 долларов. Вынесение приговора Розенфельду назначено на 9 сентября перед судьёй Крам; де ла Фе — на 31 августа перед судьёй Конбоем.

Контакты:

Federico E. Virella Jr., 212-791-1955, Офис прокурора США, Южный округ Нью-Йорка
Stephen Fishbein, 212-791-1978, Офис прокурора США, Южный округ Нью-Йорка
Betty Conkling, 212-466-4400, Секретная служба США
Joseph Valiquette Jr., 212-335-2715, Федеральное бюро расследований

Примечание редактора: Полный текст обвинительного заключения объёмом 23 страницы можно найти в Computer Underground Digest (CUD), выпуск 4.31 (доступен на ftp.eff.org/pub/cud/cud).

Кембридж, Массачусетс — Electronic Frontier Foundation (EFF) выпустил заявление в связи с предъявлением MOD обвинений в предполагаемых компьютерных преступлениях.

В заявлении, в частности, говорится, что штатный советник EFF в Кембридже Майк Годвин «внимательно изучает обвинительное заключение».

Сооснователь и президент EFF Митчелл Капор заявил: «Позиция EFF в отношении несанкционированного доступа к компьютерным системам была и остаётся неизменной: это недопустимо. Тем не менее в прошлом мы уже сталкивались с ситуациями, когда обвинения, содержавшиеся в федеральных обвинительных заключениях, также оказывались ошибочными, а гражданские свободы в информационную эпоху легко нарушаются. Именно поэтому мы намерены внимательно изучить это дело с целью установления фактов».

На вопрос о том, сколько времени может занять весь судебный процесс, помощник прокурора США Фишбейн ответил: «Я действительно не могу дать точной оценки. Продолжительность периода до начала судебного разбирательства в большей мере определяется действиями стороны защиты, нежели обвинения. Это может занять от шести месяцев до года».

Федеральные власти подключились к крупному хакерскому кольцу
13 июля 1992 г.

Автор: Mary E. Thyfault (InformationWeek, стр. 15)

Правоохранительные органы снимают перчатки и подключают свои модемы в борьбе с компьютерной преступностью.

В одном из крупнейших подобных дел в истории большое федеральное жюри в Манхэттене предъявило обвинения пяти компьютерным «хакерам» — участникам группировки, именующей себя MOD, то есть «Masters of Deception» («Мастера обмана»), — по статьям о компьютерном взломе, компьютерном мошенничестве, мошенничестве с использованием средств связи, незаконном прослушивании и сговоре.

Некоторые из хакеров обвиняются в краже телефонных услуг и продаже сведений о том, как получать кредитные отчёты. Среди пострадавших (в обвинительных заключениях названы двенадцать, однако вероятно их значительно больше) — три компании типа «Baby Bell», многочисленные кредитные бюро и BankAmerica Corp.

Впервые следователи применили санкционированное судом прослушивание для мониторинга передачи данных по телефонным линиям. Это происходит на фоне безуспешных попыток ФБР добиться от Конгресса законодательного обязания телекоммуникационных компаний встроить в новые технологии облегчённые механизмы для спецслужб по перехвату данных в компьютерных системах.

По иронии судьбы, успех этого прослушивания, как полагают некоторые, может подорвать аргументы ФБР. «Они справились без того оборудования, которое якобы им необходимо», — говорит Крейг Нейдорф, основатель хакерского журнала Phrack.

В случае обвинительного приговора предполагаемым хакерам — все они моложе 22 лет — грозит до 55 лет заключения и штраф в 250 000 долларов или удвоенная сумма нанесённого ущерба либо

извлечённой прибыли. Одному из обвиняемых, уличённому во владении устройством доступа, может грозить дополнительные пять лет.

Уязвимость сетей пострадавших компаний не должна была стать сюрпризом, однако эксперты отмечают, что корпорации по-прежнему уделяют незначительное внимание вопросам безопасности. Например, несмотря на то что кредитные бюро являются частой мишенью хакеров и заявляют об укреплении защиты своих сетей, в данном случае большинство пострадавших даже не подозревали, что на них совершаются нападения, — по данным ФБР.

Двое из пострадавших — провайдер сети с добавленной стоимостью BT Tymnet и телефонная компания Southwestern Bell — приписывают себе заслугу в разоблачении хакерской сети. «Мы сыграли ключевую роль в первоначальном обнаружении их присутствия», — говорит Джон Гинассо, директор по глобальной сетевой безопасности материнской компании BT North America. «Если вы нарушаете работу нашей сети и мы вас поймаем — а мы ловим всегда, — вы пойдёте под суд».

Второй взгляд на нью-йоркские обвинения в компьютерных преступлениях
13 июля 1992 г.

Автор: John F. McMullen (Newsbytes)

НЬЮ-ЙОРК — В среду, 9 июля, я присутствовал на пресс-брифинге в здании Федерального суда Нью-Йорка, в ходе которого сотрудники правоохранительных органов изложили подробности обвинений, предъявленных пяти молодым компьютерным «хакерам». Описывая предполагаемые преступления обвиняемых, помощник прокурора США Стивен Фишбейн живописал картину заговора, в котором члены зловеще звучащей группировки под названием «Masters of Destruction» (MOD) стремились причинить хаос в телекоммуникационной системе страны.

Обвиняемым вменялось проникновение в компьютерные системы телефонных компаний, кредитных бюро, университетов и оборонных подрядчиков — Southwestern Bell, BT North America, New York Telephone, ITT, Information America, TRW, Trans Union, Pacific Bell, Вашингтонского университета, Нью-Йоркского университета, U.S. West, Learning Link, Tymnet и Martin Marietta Electronics Information and Missile Group. Им предъявили обвинения в нанесении ущерба телефонным системам, использовании университетских компьютеров для бесплатных международных звонков, копировании персональных кредитных данных и продаже их третьим лицам — длинный перечень тяжких деяний.

Непосредственная реакция на эти обвинения оказалась предсказуемо рефлекторной. Те, кто поддерживает так называемую «хакерскую» деятельность, высмеивали правительство и предъявленные обвинения, забывая, как мне кажется, что обвинения серьёзны: одному из обвиняемых грозит до 40 лет заключения и штраф в 2 миллиона долларов; другому — 35 лет и 1,5 миллиона долларов. Принимая во внимание такую перспективу, мне представляется пустой тратой сил возмущаться тем, что правительство настаивает на неправильном употреблении слова «хакер» (обвинительное заключение определяет компьютерного хакера как «человека, использующего компьютер или телефон для несанкционированного доступа к другим компьютерам»), или что в ходе следствия было применено прослушивание (по крайней мере пока я считаю, что прослушивание осуществлялось на основании действительного судебного ордера; если это не так, у адвокатов обвиняемых есть путь обжалования).

С другой стороны, те, кто традиционно поддерживает позицию правительства и корпораций, публично выражали благодарность за устранение угрозы для жизни средств связи, — не принимая во внимание, что некоторые обвинения могут быть необоснованны и обусловлены политическими соображениями.

Обе стороны, на мой взгляд, упрощают ситуацию и не уделяют должного внимания широкому спектру вопросов, поднятых обвинительным заключением. Эти вопросы варьируются от простого чёрно-белого случая мошеннического получения бесплатной телефонной связи до куда более широкой проблемы надлежащего взаимодействия технологий и правоприменения.

Наиболее однозначны обвинения, согласно которым двое из обвиняемых — Хулио Фернандес (псевд. «Outlaw») и Джон Ли (псевд. «Corrupt») — мошеннически использовали компьютеры Нью-Йоркского университета, чтобы не платить за международные звонки в Эль-Пасо (Техас) и Сиэтл (Вашингтон). Обвиняемые либо совершили эти действия, либо нет; если вина будет доказана, они должны понести соответствующее наказание (можно дискутировать, не чрезмерен ли максимум в пять лет и штраф в 250 000 долларов за каждый из пунктов, но это вопрос назначения наказания, а не предъявления обвинений).

Столь же однозначны обвинения в том, что Фернандес и/или Ли перехватывали электронные коммуникации в сетях Tymnet и Bank of America. Аналогично обвинение в том, что 4 декабря 1991 года у Фернандеса находились сотни идентификаторов пользователей и паролей Southwestern Bell, BT North America и TRW, — здесь тоже либо виновен, либо нет.

Более спорным является обвинение в сговоре всей пятёрки с целью «получения доступа к компьютерным системам и установления над ними контроля для повышения своего образа и престижа в среде других компьютерных хакеров; для преследования и запугивания соперников-хакеров и неугодных лиц; для получения телефонных, кредитных, информационных и прочих услуг без оплаты; а также для получения паролей, номеров счетов и иных ценных сведений с целью их продажи».

В подтверждение этого обвинения заключение приводит 26 «открытых действий» (пронумерованных от A до Z). В данном разделе перечислены многочисленные телефонные переговоры между некоторыми из обвиняемых, однако имя Пола Стайры (псевд. «Scorpion») упоминается лишь дважды, причём оба раза с датой «около 24 января 1990 года» — за полных 16 месяцев до следующего хронологического эпизода. Более того, Стайра нигде не фигурирует как участник перехваченных переговоров — и больше не упоминается ни разу! Я с трудом могу поверить, что на основании этих обвинений его можно считать участником преступного сговора с кем-либо из остальных обвиняемых.

Кроме того, некоторые обвинения в рамках статьи о сговоре явно несоразмерны друг другу. Марку Абене (псевд. «Phiber Optik») вменяется хранение собственнических технических руководств BT North America, тогда как Ли и Фернандес обвиняются в том, что за несколько сотен долларов предоставили некоему Мортону Розенфельду как информацию о незаконном доступе к кредитным бюро, так и действующий аккаунт и пароль TRW; Розенфельд впоследствии незаконно получил кредитные отчёты на 176 граждан и продал их частному детективу (сам Розенфельд, обвиняемый отдельно, признал вину и назвал «Хулио» и «Джона» теми, кто снабдил его информацией). В обвинениях я нигде не обнаружил указаний на то, что Абене, Стайра или Элиас Ладопулос вступали в сговор с Ли или Фернандесом или иным образом побуждали их продавать информацию о кредитных бюро третьим лицам.

Ещё один тревожный момент — утверждение о том, что Фернандес, Ли, Абене и «другие лица, которым они оказывали помощь», совершили различные компьютерные действия, «причинившие Southwestern Bell ущерб приблизительно в 370 000 долларов». По словам помощника прокурора Фишбейна, эту цифру рассчитала сама Southwestern Bell, включив в неё «расходы на поиск и восстановление компьютерных программ и иных данных, изменённых или повреждённых, расходы на установление источника несанкционированного вторжения, а также расходы на приобретение нового оборудования и средств защиты, необходимых для предотвращения дальнейшего несанкционированного доступа со стороны обвиняемых и лиц, которым они оказывали помощь».

Хотя существует прецедент возмещения таких расходов (дело Риггса, Дардена и Гранта в Атланте признало ответственность обвиняемых за подобные затраты), многие считают такой подход в корне неверным. Если человека обнаружили в чужом доме без разрешения, ему предъявляют соответствующие обвинения — незаконное проникновение, вторжение, взлом, смотря какой закон применяется; однако ему не выставляют счёт за установку сигнализации или более надёжных замков, чтобы никто другой не вошёл незаконно.

Когда я обсудил этот вопрос с нью-йоркским менеджером по ИТ, склонным занимать жёсткую позицию против злоумышленников, он сказал, что вспышка новых преступлений нередко влечёт за собой использование новых технических устройств — как, например, повсеместная установка металлодетекторов в аэропортах в 1970-х. Хотя он имел в виду это как обоснование ответственности, аналогия, напротив, поддерживает противоположную позицию. Угонщиков самолётов преследуют по всевозможным серьёзным статьям; однако никто никогда не возлагал на них расходы по установке металлодетекторов или жалованье дополнительных воздушных маршалов.

Я думаю, авиационная аналогия также наглядно иллюстрирует, что можно одновременно поддерживать оправданные санкции за доказанные преступления и возражать против неразумных — слишком часто в подобных дискуссиях наблюдатели выбирают одну обоснованную позицию в ущерб другой, не менее обоснованной. На мой взгляд, нет никакого противоречия в том, чтобы одновременно считать: кредитные агентства обязаны обеспечивать максимально высокий уровень защиты собранных ими данных И что лица, вторгающиеся в кредитные базы данных, сколь бы надёжными те ни были, несут ответственность за свои действия. Мы давно уже не принимаем аргумент о том, что злоумышленники «лишь демонстрируют незащищённость этих хранилищ нашей информации». Все мы знаем, что отсутствие безопасности — это скандал; однако данный факт не оправдывает преступного поведения (и должно быть очевидно, что продажа электронных «отмычек», позволяющих копировать и реализовывать кредитные отчёты, не является общественной услугой).

Последний вопрос, заслуживающий серьёзного рассмотрения, — использование обвинительного заключения как инструмента в текущей политической дискуссии вокруг предложения ФБР о «цифровой телефонии». Объявляя об обвинениях, прокурор США Обермайер заявил, что данное расследование стало «первым следственным применением санкционированного судом прослушивания для получения переговоров и данных компьютерных хакеров». Он подчеркнул, что эта процедура была необходима для следствия, и добавил: «Это доказывает, на мой взгляд, способность федерального правительства бороться с преступностью по мере её распространения в новые технологические области». Он также указал, что перехват данных стал возможен лишь потому, что материал был в аналоговой форме, и добавил: «Большинство новых технологий существуют в цифровом виде, и в Конгрессе находится на рассмотрении законопроект, добивающийся поддержки телекоммуникационных компаний для того, чтобы федеральное правительство могло, при наличии судебной санкции, перехватывать цифровые передачи. Многие из вас, возможно, читали в газетах о лазерных передачах по оптоволокну как о грядущем методе телекоммуникаций. Федеральное правительство нуждается в помощи Конгресса и, собственно, самих телекоммуникационных компаний для обеспечения возможности перехвата цифровых коммуникаций».

Предложение ФБР подверглось жёсткой критике со стороны Американского союза гражданских свобод (ACLU), Electronic Frontier Foundation (EFF) и Computer Professionals for Social Responsibility (CPSR): по их мнению, оно представляет собой попытку впервые закрепить в законодательстве уголовные расследования как обязанность коммуникационных компаний — ответственность, которая, по их убеждению, принадлежит исключительно правоохранительным органам. Критики также утверждают, что предложение затормозит развитие технологий и вынудит разработчиков «упрощать» свои продукты, встраивая в них запрашиваемые механизмы перехвата. ФБР, в свою

очередь, настаивает на том, что речь идёт лишь о сохранении нынешних возможностей ведомства в условиях наступающих технологий.

Каковы бы ни были достоинства позиции ФБР, представляется, что обвинения либо не были бы предъявлены в это время, либо, по меньшей мере, не были бы представлены с такой помпой, если бы не стремление заручиться поддержкой pending-законодательства. Пресс-конференция оказалась крупнейшим событием подобного рода со времён пресс-конференции «Операции Sun Devil» в мае 1990 года в Финиксе (Аризона). Тогда нас поразили обвинениями «хакеров» в угрозе жизни людей через нарушение работы больниц и участии в общенациональном заговоре в 13 штатах. На этот раз речь шла о группе нью-йоркских подростков, якобы занимавшихся мелким воровством, использовавших университетские компьютеры без разрешения и совершивших ряд других действий, которые Обермайер охарактеризовал как «антиобщественное поведение», — далеко не столь громкое дело!

Речь идёт не о том, чтобы преуменьшить серьёзность обвинений, — вопрос в уместности помпезности. На конференции присутствовали высокопоставленные сотрудники Министерства юстиции, ФБР и Секретной службы. Опытные криминальные репортёры Нью-Йорка говорят мне, что масштаб предполагаемого ущерба в данном деле обычно не требует подобного театра. Репортёр New York Daily News Алекс Микелини публично сказал Обермайеру: «В целом то, что вы описали, — кроме продажи кредитной информации — звучит как большая шутка, большая её часть». Ответ Обермайера: «Ну что же, наверное, это можно назвать шуткой, но это действительно федеральное преступление — позволять людям без разрешения рыться в чужих данных, к которым у них нет доступа; и, как я ещё раз укажу, взломщик не может быть вашим экспертом по безопасности. Он может оказаться внутри и посмеяться над вами, когда вы приходите домой и видите, что ваш замок не особо надёжен, — но я думаю, что, окажись вы жертвой такого визита, вы были бы несколько раздражены». Хочется надеяться, что с инициативой ФБР связана лишь помпезность вокруг обвинений, но не сами обвинения.

В качестве отступления: двое сотрудников правоохранительных органов, с которыми я беседовал, отметили, что фраза «первое следственное применение санкционированного судом прослушивания для получения переговоров и данных компьютерных хакеров», при всей своей вероятной истинности, создаёт впечатление, будто это первый случай перехвата передачи данных как такового. По их словам, это далеко не так: в последние годы правоохранительные органы неоднократно перехватывали данные и факсимильные сообщения.

Я в разной мере знаком с каждым из обвиняемых. Лучше всего я знаю Phiber Optik, который участвовал в панельных дискуссиях со мной и сотрудниками правоохранительных органов по вопросам так называемой хакерской преступности. Он также появлялся на различных радио- и телепередачах на те же темы. Его высокий публичный профиль раздражал кое-кого в правоохранительных кругах. Хочется надеяться, что это раздражение никак не повлияло на его обвинение.

Присутствие Phiber в этих дискуссиях я нахожу чрезвычайно ценным — и по содержанию, и потому, что его появление привлекает аудиторию, которая иначе, пожалуй, никогда не услышала бы голоса Дональда Делани, Майка Годвина, Дороти Деннинг и других, рассматривающих те же проблемы с совершенно иных позиций. Хотя в своих выступлениях он говорил, что «идёт на риск ради получения знаний», он всегда отрицал причастность к вандализму и критиковал тех, кто им занимается. Он также называл тех, кто занимается «кардингом» и тому подобным, преступниками — и это звучало не только в ходе панельных дискуссий, но и в тех случаях, когда он выступал в качестве приглашённого лектора в моём курсе «Коммуникации» в New School for Social Research в Нью-Йорке. На этих занятиях он рассказывал об истории телефонных коммуникаций так, что удерживал внимание профессиональной аудитории более двух часов.

Мои впечатления о Phiber и остальных, разумеется, не являются гарантией их невиновности по данным обвинениям, однако должны восприниматься как моё личное свидетельство того, что перед нами — не закоренелые уголовники, которых стоило бы бояться тёмной ночью.

Подводя итог: рефлекторные реакции следует отставить, а вдумчивый анализ — поставить во главу угла! Мы должны настаивать на соразмерном наказании для нарушителей закона — а это означает ни потворство «исследовательским» мотивам, ни допущение непомерных санкций. Мы должны требовать, чтобы компании, собирающие данные о нас, надлежащим образом их защищали и несли ответственность за несоблюдение этого требования. И мы не должны отвлекаться на поддержку или противодействие предложению ФБР в Конгрессе — это требует отдельного анализа и никак не связано ни с виновностью или невиновностью этих молодых людей, ни с надлежащим наказанием в случае установления их вины.

Нью-йоркские хакеры заявили о своей невиновности 17 июля 1992 г.

Нью-Йорк — На заседании федерального суда в четверг, 16 июля, пятеро нью-йоркских «хакеров», недавно обвинённых в предполагаемом несанкционированном доступе к компьютерным системам, все заявили о своей невиновности и были освобождены после подписания каждым личного залогового обязательства (PRB) на 15 000 долларов для обеспечения явки в суд.

В ходе слушания дело было передано судье Федерального окружного суда Ричарду Оуэну, которому предстоит председательствовать на процессе; назначена предварительная встреча судьи со сторонами.

Чарльз Росс, адвокат Джона Ли, сообщил Newsbytes: «Джон Ли заявил о своей невиновности, и мы намерены энергично и агрессивно защищать его от предъявленных обвинений».

Росс также описал порядок рассмотрения дела: «Мы встретимся с судьёй, и он утвердит график раскрытия доказательств и подачи ходатайств. Сторона защиты должна будет ознакомиться с доказательной базой, собранной обвинением, прежде чем подавать обоснованные ходатайства; первая встреча носит сугубо организационный характер».

Мажори Пирс, адвокат Стайры, сказала Newsbytes: «Господин Стайра заявил о своей невиновности и намерен сохранять эту позицию. Мне жаль видеть, как правительство привлекает к суду 22-летнего студента за действия, которые он предположительно совершил в 19 лет».

Условия подписанного обвиняемыми залогового обязательства предписывают им оставаться в пределах континентальной части Соединённых Штатов. Запрашивая данное обязательство, помощник прокурора США Стивен Фишбейн охарактеризовал обвинения как серьёзные и просил установить залог в 15 000 долларов с условием совместного подписания поручительства родителями. Абене, Фернандес и Ли через своих адвокатов согласились с залогом на этих условиях; адвокаты Ладопулоса и Стайры ходатайствовали об отказе от залога для своих клиентов, указав, что те были доступны для властей по первому требованию на протяжении более года. После рассмотрения судьёй аналогичный залог в 15 000 долларов был установлен и для Ладопулоса, и для Стайры, однако без требования о поручительстве.

Молодые хакеры из рабочих кварталов обвинены в высокотехнологичных преступлениях 23 июля 1992 г.

Авторы: Mary B.W. Tabor и Anthony Ramirez (The New York Times, стр. B1, B7)

Компьютерные таланты с характером

Глубокой ночью в рабочих кварталах Нью-Йорка молодые люди с псевдонимами Acid Phreak и Outlaw, сгорбившись, сидели перед светящимися мониторами, обмениваясь электронными ключами к сложным информационным системам. Они называли себя «Мастерами обмана». Их миссия: доказать свою мощь в теневом компьютерном подполье.

Компульсивные и конкурентные, они разыгрывали киберверсию «Вестсайдской истории» — хвастались, проникали в телефонные системы, вытаскивали конфиденциальные кредитные отчёты, чтобы продемонстрировать свою дерзость и позлить других хакеров. Частой мишенью была Legion of Doom — хакерская группа, названная в честь шайки злодеев из комиксов. Это противостояние приобрело классовые и этнические оттенки: разношёрстная нью-йоркская группа бросала вызов традиционному образу юного пригородного компьютерного гения.

Однако федеральные прокуроры утверждают, что члены MOD вышли далеко за рамки невинных шалостей.

Федеральные обвинения

16 июля пятеро молодых людей, которых прокуроры называют членами MOD, заявили о своей невиновности по федеральным обвинениям во взломе некоторых наиболее защищённых компьютеров страны и краже конфиденциальных данных — кредитных отчётов, часть которых была впоследствии продана частным сыщикам. Прокуроры называют это одним из наиболее масштабных хищений компьютерной информации из когда-либо зафиксированных.

В обвинительном заключении говорится, что обвиняемые проникали в компьютерные системы Southwestern Bell, TRW Information Services и других компаний «для повышения своего образа и престижа в среде других компьютерных хакеров; для преследования и запугивания соперников-хакеров и неугодных им людей; для получения телефонных, кредитных, информационных и прочих услуг без оплаты; а также для получения паролей, номеров счетов и иных ценных сведений с целью их продажи другим».

С помощью модемов, связывающих их терминалы с другими компьютерами по обычным телефонным линиям, молодые хакеры годами устраивали пакости. Но по мере того как страна всё больше зависит от обширных сетей мощных компьютеров, а персональные компьютеры становятся быстрее и дешевле, потенциал для бедствий резко возрос. Для примера: Роберт Таппан Моррис, студент Корнелла, в 1988 году запустил программу, которая парализовала несколько тысяч компьютеров по всей стране.

Разношёрстная компания

Но мир компьютерных хакеров меняется. В отличие от типичных хакеров прошлого — обеспеченных пригородных юношей, чьи родители могли позволить себе дорогостоящее оборудование, — «Мастера обмана» представляют собой разношёрстный срез рабочего Нью-Йорка: чернокожие, латиноамериканцы, греки, литовцы и итальянцы. Свои пакости они творят зачастую с помощью самых дешёвых компьютеров.

Одному из молодых людей, 21-летнему Джону Ли, известному под псевдонимом Corrupt, дреды подстрижены в короткие «пучки»; он живёт с матерью в ветхом доме без лифта в Бедфорд-Стайвесанте, Бруклин. Он переходил из одной программы для одарённых учеников в другую, а в одиннадцатом классе бросил школу. Scorpion — 22-летний Пол Стайра из Куинса — окончил школу Thomas A. Edison High School лучшим учеником. Outlaw — Хулио Фернандес, 18 лет, из Бронкса — начал изучать компьютеры ещё в начальной школе.

Познакомились они не на уличных углах, а через компьютерные доски объявлений, служившие для обмена сообщениями и программами.

Не имея на бордах никаких опознавательных знаков, кроме псевдонимов и незаурядных способностей, молодые люди обнаружили, что компьютер — великий демократический уравнитель.

Вопрос наживы

Возможно, в новой волне хакеров есть ещё одно отличие. Тогда как традиционная хакерская этика запрещает бороздить компьютерные системы ради прибыли, некоторые новые хакеры менее идеалистичны. «Те, кто так говорит, — сказал один бывший хакер, друг MOD, настоявший на анонимности, — наверное, имеют богатых родителей. Когда что-то ценное попадает в руки, нужно на этом зарабатывать».

Ли, Фернандес, Стайра и ещё двое, описанных как члены MOD, — 20-летний Марк Абене (Phiber Optik) и 22-летний Элиас Ладопулос (Acid Phreak), оба из Куинса, — обвинены в компьютерном взломе, компьютерном и телекоммуникационном мошенничестве, незаконном прослушивании и сговоре. Им грозят огромные штрафы и до пяти лет заключения по каждому из 11 пунктов обвинения.

Молодые люди по совету адвокатов отказались от интервью.

По словам прокуроров, они не знают точно, когда и как юношеские шалости переросли в серьёзные преступления. Другие хакеры говорят, что неприятности начались, возможно, вполне невинно — как компьютерная война с этническим и классовым подтекстом.

«Мастера обмана» родились из конфликта с Legion of Doom — группой, сформировавшейся к 1984 году, в число членов которой в итоге вошли три техасца, один из них, Кеньон Шульман, — сын хьюстонской светской дамы Кэролин Фарб.

Изгнание из Легиона

Абене в своё время проголосованием был принят в Legion. Но когда он начал раздражать остальных членов группы своим нью-йоркским хвастовством и нежеланием делиться информацией, его изгнали, по словам членов Legion.

Тем временем один из хакеров, использовавший компьютерную вечеринку-линию из Техаса, оскорбил Ли, который является чернокожим, расистским эпитетом.

К 1989 году оба нью-йоркца примкнули к новой группе — MOD, основанной Ладопулосом. Они поклялись вытеснить своих соперников из Легиона как «новую элиту».

«Это как любой другой 18–19-летний парень, который ходит и знает, что умеет делать что-то лучше всех остальных», — сказал Майкл Годвин, знакомый с несколькими из обвиняемых и являющийся юристом Electronic Frontier Foundation из Кембриджа (Массачусетс), оказывающего юридическую помощь хакерам. «Они оскорбительно высокомерны».

Хакерские группы, как правило, взлетают и распадаются в течение полугода — по мере того как участники уходят в колледжи, заводят подруг или, как выразился один бывший хакер, «начинают жить нормальной жизнью». Но MOD продолжал пополнять ряды на ежемесячных встречах в атриуме здания Citicorp в Манхэттене и на компьютерной доске объявлений под названием Kaos. Согласно истории группы, хранившейся в компьютерной сети, они упивались «озорными шалостями», нередко направленными против техасских соперников, и между двумя группами вспыхивала перебранка.

Техасско-нью-йоркские стычки

В июне 1990 года трое техасских членов Legion — в том числе Шульман, Крис Гоггэнс и Скотт Часин — основали Comsec Data Security, компанию, помогающую предприятиям защищаться от вторжений других хакеров.

Опасаясь, что техасцы действуют как полицейские осведомители, члены MOD обвинили своих соперников в клевете на форумах. Несколько участников MOD, в том числе Абене, стали объектами налётов Секретной службы, и члены MOD считали виновными техасцев — на что те отвечали «без комментариев».

Стычки приобрели и расовый оттенок. Когда Ли написал историю MOD и оставил её в сети, Гоггэнс переписал её в виде пародии на сленге.

Фраза «В начале 1987 года в США и особенно в Нью-Йорке прошла целая серия арестов» превратилась в «В начале той части 1987 года, в Амерыке и особо в Нью-Йорке, было немеряно арестов».

Гоггэнс сказал, что это не было задумано как расистская атака на Ли. «Это был просто хороший способ задеть его за живое», — объяснил он.

Раскрытие личностей

Деятельность MOD, согласно обвинительному заключению и другим хакерам, стала расширяться.

В отличие от большинства представителей «старшего поколения» хакеров, любивших беспечно кататься по системам, нью-йоркцы начали использовать полученную информацию для преследования и запугивания других, по словам прокуроров. В сети появлялось всё подряд: домашние адреса, номера кредитных карт, места работы, настоящие имена хакеров — пожалуй, самое страшное табу.

В обвинительном заключении утверждается, что прошлой осенью Ли и Фернандес вели разговор, в котором обсуждали получение информации о том, как изменять кредитные досье TRW, чтобы «разрушать жизни людей или делать из них святых».

По словам прокуроров, молодые люди также охотились за информацией, которую можно было продать, хотя обвинительное заключение не конкретизирует, что именно и было ли что-либо продано. Единственные подобные сведения поступают из другого дела ранее в этом месяце: двое других нью-йоркских хакеров — Мортон Розенфельд, 21 год, из Бруклина, и Альфредо де ла Фе, 18 лет, из Манхэттена — признали вину в сговоре с использованием паролей и иных устройств доступа, полученных от MOD. Они сообщили, что заплатили группе «несколько сотен долларов» за пароли для получения кредитных отчётов, а затем перепродали информацию «за несколько тысяч долларов» частным сыщикам.

Внимание СМИ

Конкуренция за внимание СМИ также обострилась. Бывшие члены Legion в Comsec превратились в любимчиков медиа — о них выходили статьи в Time и Newsweek. Абене и Ладопулос также появлялись на телевидении и в журналах, провозглашая своё право зондировать компьютерные системы при условии, что они не наносят ущерба.

В одном широко освещавшемся инциденте во время форума по компьютерам и конфиденциальности 1989 года, организованного журналом Harper's, Джон Перри Барлоу — журналист-фрилансер и поэт-текстовик The Grateful Dead — сошёлся в полемике с Абене, он же Phiber Optik. Барлоу назвал молодого хакера «панком».

По словам Барлоу — версия, которую Абене отказывается ни подтверждать, ни опровергать, — Абене ответил тем, что «скачал» кредитную историю Барлоу и отобразил её на экранах компьютеров самого Барлоу и других пользователей сети.

Затишье в противостоянии

«Я бывал в барах для деревенщин с волосами до плеч, под стражей в состоянии наркотического опьянения и в Гарлеме после полуночи — но никто никогда не вселял в меня такого страха, как Phiber Optik в тот момент», — написал Барлоу. «Для американца среднего класса кредитный

рейтинг стал почти тождественен его свободе».

В последние месяцы, по словам хакеров, война поутихла. Comsec закрылась, и несколько «Мастеров обмана» лишились компьютеров после налётов Секретной службы.

В прошлом году Абене признал себя виновным по обвинению в административном правонарушении, возникшем в результате налётов. Накануне своего ареста в этом месяце он прочитал гостевую лекцию по компьютерам в New School for Social Research.

По словам Ли, он подрабатывает стенд-ап комиком и числится студентом Бруклинского колледжа по специальности кинопроизводство.

Стайре не хватает трёх зачётных единиц до диплома по информатике в Polytechnic University в Бруклине. Фернандес надеется поступить этой осенью в Technical Computer Institute на Манхэттене. Ладопулос учится в Queens Community College.

Дата начала судебного процесса не назначена.

Но сражения, судя по всему, ещё не закончены. Через несколько дней после предъявления обвинений один из членов Legion сообщил, что получил на компьютере сообщение от Абене. Привычно саркастическое, оно заканчивалось словами: «Целую-целую».

[Примечание редактора: В статье были помещены фотографии Phiber Optik, Scorpion, Corrupt и Outlaw.]

Разочарованные хакеры, возможно, помогли федералам в деле MOD
20 июля 1992 г.

Автор: James Daly (ComputerWorld, стр. 6)

НЬЮ-ЙОРК — Хакеры начинают полицировать самих себя? Пятеро недавно обвинённых во взломе десятков сложных компьютерных систем на протяжении последних двух лет могли быть сданы другими хакерами, уставшими от склонности этой группы к разрушению и мстительности, — так утверждают представители хакерского сообщества.

Арест обвиняемых, которых сотрудники федеральных правоохранительных органов называли членами конфедерации, именовавшей себя по-разному — «Masters of Deception» и «Masters of Disaster» (MOD), — вызвал ликование в тех кругах, где группу знали как злобный маргинальный элемент.

«Некоторые из этих ребят были настоящей занозой», — сказал один источник, попросивший сохранить анонимность из опасения, что неарестованные члены MOD затеют месть. «Они использовали свои навыки для преследования других — а это совсем не то, для чего существует хакерство. MOD приходил с установкой "вы будете нас уважать", и это никому не нравилось».

«В последние несколько месяцев на [досках объявлений] было много ворчания насчёт этих ребят», — добавил другой.

В одном из эпизодов члены MOD предположительно организовали непрерывный автодозвон с модема компьютера Луисвиллского университета (Кентукки) на домашний номер участника хакерского форума, отказавшегося предоставить им расширенные права доступа. Аналогичная угроза поступала и в Мэриленде.

В обвинительном заключении обвиняемые обвиняются в ведении разговора в начале ноября 1991 года, в котором они искали способы добавлять и удалять записи о просроченных кредитах «чтобы разрушать жизни людей... или делать их похожими на святых». В отличие от многих других

хакерских организаций, члены MOD договорились делиться важной компьютерной информацией исключительно между собой, но не с другими хакерами.

Власти молчат

Кто именно помогал ФБР, Секретной службе и Офису генерального прокурора США подготовить дело против группы — до сих пор неизвестно. Помощник прокурора США Стивен Фишбейн не говорит. Он подтвердил, что расследование в отношении MOD началось в 1990 году, однако отказался уточнить, как и почему оно было возбуждено и кто принимал в нём участие. Сотрудники ФБР и Секретной службы также хранили молчание.

Ряд наблюдателей заявил: если обвинения соответствуют действительности, эти люди вовсе не были настоящими «хакерами».

«Хакерство — это нечто, совершаемое в духе творческой игривости, а люди, взламывающие системы безопасности компьютеров, — не хакеры, они преступники», — сказал Ричард Столлман, президент базирующегося в Кембридже (Массачусетс) Free Software Foundation — общественной благотворительной организации, разрабатывающей свободное программное обеспечение. На одном из компьютеров фонда были удалены несколько файлов хакером, которого некоторые связывали с MOD.

Хакерам из MOD предъявлено обвинение во взломе компьютерных систем нескольких региональных телефонных компаний, компаний из списка Fortune 500 (в том числе Martin Marietta Corp.), университетов и кредитных организаций, таких как TRW, Inc., у которой якобы было похищено 176 кредитных отчётов на потребителей и продано частным сыщикам. Обвинительное заключение из 11 пунктов обвиняет обвиняемых в компьютерном мошенничестве, компьютерном взломе, мошенничестве с использованием средств связи, незаконном прослушивании и сговоре.

Однако некоторые хакеры считают, что предъявленные обвинения — всё равно что давить муравьёв кувалдой. «Эти ребята, возможно, вели себя как идиоты, но это был тупой способ с ними разделаться», — сказал Эммануэль Голдстейн, редактор 2600, ежеквартального журнала для хакерского сообщества, базирующегося в Middle Island (Нью-Йорк).

Давние хакеры рассказывают, что MOD стремился заполнить вакуум, образовавшийся после того, как Legion of Doom начал распадаться в конце 1989 — начале 1990 года после ряда арестов в Атланте и Техасе. Федеральные правоохранительные органы описывали Legion of Doom как группу примерно из 15 компьютерных энтузиастов, чьи члены перенаправляли звонки, похищали и изменяли данные и нарушали работу телефонных служб.

Bellcore угрожает журналу 2600 судебным иском
15 июля 1992 г.

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN               Phrack World News             PWN
PWN                                             PWN
PWN            Issue 40 / Part 3 of 3           PWN
PWN                                             PWN
PWN         Compiled by Datastream Cowboy       PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Автор: Datastream Cowboy

НИЖЕСЛЕДУЮЩЕЕ ЗАКАЗНОЕ ПИСЬМО БЫЛО ПОЛУЧЕНО ЖУРНАЛОМ 2600. МЫ ПРИВЕТСТВУЕМ ЛЮБЫЕ КОММЕНТАРИИ И/ИЛИ ИНТЕРПРЕТАЦИИ.

Leonard Charles Suchyta
Главный юрисконсульт
Вопросы интеллектуальной собственности

Emanuel [sic] Golstein [sic], редактор
2600 Magazine
P.O. Box 752
Middle Island, New York 11953-0752

Уважаемый г-н Голстейн,

Нам стало известно, что вы каким-то образом получили и опубликовали в зимнем выпуске журнала 2600 Magazine за 1991–1992 год фрагменты определённых внутренних документов, являющихся собственностью Bellcore.

Настоящим письмом мы официально уведомляем вас о том, что если в будущем вы (или ваш журнал) получите, опубликуете или иным образом раскроете какую-либо информацию или документацию Bellcore, которая (i) даёт вам основания полагать, что она является собственностью Bellcore или не была сделана ею общедоступной, либо (ii) имеет пометку «proprietary» («собственность компании»), «confidential» («конфиденциально»), «restricted» («ограниченный доступ») или любую иную пометку, указывающую на права собственности Bellcore, — Bellcore будет настойчиво добиваться всех доступных ей правовых мер, включая, помимо прочего, судебный запрет и возмещение денежного ущерба, в отношении вас, вашего журнала и его источников.

Надеемся, что вы в полной мере понимаете позицию Bellcore по данному вопросу.

С уважением,

LCS/sms

LCS/CORR/JUN92/golstein.619

Ответ Эммануэля Голдстейна

Нижеследующий ответ был направлен в Bellcore. Поскольку мы полагаем, что к этому моменту они его уже получили, мы делаем его достоянием общественности.

Emmanuel Goldstein
Редактор, 2600 Magazine
PO Box 752
Middle Island, NY 11953

20 июля 1992 г.

Leonard Charles Suchyta
LCC 2E-311
290 W. Mt. Pleasant Avenue
Livingston, NJ 07039

Уважаемый г-н Сучита,

Нам жаль, что информация, опубликованная в зимнем выпуске журнала 2600 за 1991–92 год, вас беспокоит. Поскольку вы не указываете, к какой именно статье предъявляете претензии, мы вынуждены предположить, что речь идёт о нашем материале, посвящённом встроенным уязвимостям конфиденциальности в телефонной инфраструктуре, который появился на странице 42. В этой статье мы цитировали внутренний меморандум Bellcore, а также документы Bell Operating Company. Это не первый раз, когда мы это делаем. И не последний.

Мы понимаем, что для вас должно быть неприятно, когда такой журнал, как наш, публикует потенциально компрометирующую информацию подобного рода. Но как журналисты мы несём определённое обязательство, которое нельзя отбросить каждый раз, когда какая-то крупная и влиятельная организация бывает раздражена. Это обязательство побуждает нас сообщать факты нашим читателям, которые живо интересуются данной темой. Если, как это нередко бывает, к нам попадают документы, меморандумы и/или отдельные сведения в иных формах, мы имеем полное право сообщать об их содержании. Если вы видите изъян в этой логике, ваши претензии адресованы не нам, а самой концепции свободной прессы.

И как юрист, специализирующийся на праве интеллектуальной собственности, вы знаете, что нельзя добросовестно утверждать, будто простое проставление на документе штампа «proprietary» или «secret» автоматически делает его коммерческой тайной или конфиденциальной информацией. В отсутствие конкретных пояснений, опровергающих обратное, мы вынуждены считать, что информация об общественно значимой телефонной системе и инфраструктуре представляет публичный интерес, и что Bellcore едва ли сможет доказать в суде, что какая-либо информация в нашем журнале может принести пользу конкурентам Bellcore — если, конечно, таковые у неё вообще имеются.

Если вы всё же решите оспорить наше конституционное право на распространение важной информации о телефонной инфраструктуре, мы будем вынуждены ответить, прибегнув ко всем доступным нам правовым средствам, включая санкции, предусмотренные федеральным и государственным законодательством, а также нормами гражданского судопроизводства. Кроме того, мы будем вынуждены предать огласке ваше использование судебных исков и угроз правовых действий в целях запугивания и давления.

С уважением,

Emmanuel Goldstein

Раскрытая дыра в телефонной сети вызывает гнев Bellcore 24 июля 1992 г.

Взято из Communications Daily (стр. 5)

Каждый может прослушать ваш телефон

Серьёзная дыра в безопасности телефонной сети создаёт функцию мониторинга в режиме «самообслуживания», позволяющую кому угодно прослушивать любой телефонный разговор по своему выбору. Уязвимость связана с функцией Busy Line Verification (BLV) — проверки занятой линии, — которая позволяет телефонным компаниям «вклиниваться» в разговор в любое время. Чаще всего BLV используется операторами, которые вторгаются в разговор, чтобы сообщить абоненту о срочном сообщении. Но эта функция может быть использована любым, кто знает о слабости сети, для организации стихийного «прослушивания» и мониторинга переговоров, заявил Эммануэль Голдстейн, редактор журнала 2600 Magazine, опубликовавшего соответствующую статью в зимнем выпуске 1991 года.

Журнал 2600 Magazine известен тем, что находит и разоблачает уязвимости телекоммуникационных систем. Своё название он получил в честь частоты свистка, когда-то прилагавшегося к хлопьям Cap'n Crunch: один известный хакер обнаружил, что если свистнуть в телефонную трубку, можно получить доступ к открытой линии 800. Телефонные компании с тех пор устранили эту проблему.

Риски безопасности описаны в статье «U.S. Phone Companies Face Built-In Privacy Hole», в которой цитируется внутренний меморандум Bellcore и документы Bell Operating Co.: «'Существенная и изощрённая уязвимость', способная затронуть безопасность и конфиденциальность BLV». В статье подробно описывается, как после выполнения четырёх шагов любая линия оказывается доступна для тайного прослушивания. В одном из документов, полученных 2600, говорилось: «Нет доказательств того, что хакерскому сообществу известно об этой уязвимости».

Когда Bellcore узнала о статье, она направила журналу жёсткое письмо с угрозой судебного иска. В письме говорилось, что если в будущем журнал «получит, опубликует или иным образом раскроет любую информацию Bellcore», организация «будет настойчиво добиваться всех доступных ей правовых мер, включая, помимо прочего, судебный запрет и возмещение денежного ущерба». Леонард Сучита, главный юрисконсульт Bellcore по вопросам интеллектуальной собственности, заявил, что документы, находящиеся в распоряжении журнала, «являются собственностью компании» и представляют собой «коммерческую тайну», принадлежащую Bellcore и её участникам — региональным компаниям Bell (RBOC). По его словам, документы «имеют пометку 'Proprietary'», и «закон говорит, что вы не можете игнорировать эту пометку — это её [Bellcore] собственность». Сучита объяснил, почему Bellcore так долго не реагировала на публикацию: «Думаю, что статья, поскольку мы не являемся подписчиками, была доведена до нашего сведения третьей стороной». Он также отметил, что это первый известный ему случай, когда журнал публикует подобную информацию Bellcore.

Однако Голдстейн в ответном письме заявил: «Это не первый раз, когда мы это делаем. И не последний». По его словам, Bellcore пытается его запугать, «но на этот раз они нарвались не на тех». Голдстейн настаивал на том, что документы были переданы его журналу в виде утечки: «Хотя мы не распространяем сами документы, мы сообщаем о том, что в них содержится». Сучита возразил, что журнал обязан соблюдать пометку на документах. По его словам, судебная практика свидетельствует: право на публикацию информации зависит от того, была ли она «получена законным путём. Если на ней есть пометка, довольно сложно утверждать, что она получена законно».

Голдстейн ответил, что лишь предавал огласке то, что уже было известно: существует известный риск для конфиденциальности из-за уязвимости BLV: «Если мы что-то узнаём, наш первый инстинкт — рассказать об этом людям. Мы не замалчиваем информацию». По его словам, информация об уязвимостях телефонной сети «касается всех». То, что Bellcore не хочет, чтобы все знали о её недостатках и недостатках телефонной сети, — это едва ли повод подавлять эту

информацию, заявил Голдстейн. «Все должны знать, могут ли их телефонные разговоры прослушиваться».

Сучита заявил, что чтобы считаться «ценной», информация «не обязательно должна быть сверхценной» — как запатентованная программа, «на разработку которой вы потратили миллионы долларов». По его словам, информация «вполне может быть вашей собственной информацией, которая даёт кому-то преимущество или добавочную стоимость, которой у него не было бы, если бы он не взял её у вас». Голдстейн сказал, что он «с пониманием» относится к озабоченности Bellcore, но «факт в том, что даже когда подобные уязвимости раскрываются, [телефонные компании] ничего с ними не делают». Он сослался на недавние обвинительные заключения в Нью-Йорке, где компьютерные хакеры манипулировали телефонной системой, эксплуатируя уязвимости, о которых его журнал писал давным-давно. «Есть ли вообще хоть какая-то безопасность [в сети]? — сказал он. — Вот вопрос, который мы должны себе задать».

Письмо от Bellcore вызвало поток откликов из компьютерного сообщества, когда Голдстейн опубликовал его в электронной компьютерной конференции. Юристы, специализирующиеся на компьютерном праве, приняли сторону журнала. Адвокат Лэнс Роуз заявил: «Не существует никакого 'права на секретность' в общем смысле... Даже если документ помечен как 'конфиденциальный', это не означает, что он был передан вам с условием сохранения конфиденциальности — а именно это является ключевым вопросом». Майкл Годвин, главный юрисконсульт Electronic Frontier Foundation, правозащитной организации компьютерного сообщества, сказал: «Коммерческие тайны могут считаться собственностью, но только если они действительно являются коммерческими тайнами. Конфиденциальная информация (в определённом смысле) может считаться собственностью при наличии нарушения доверительных обязанностей». Оба юриста согласились с тем, что журнал действовал в рамках своих прав, публикуя эту информацию. «Если Эммануэль никоим образом не участвовал в поощрении или содействии извлечению документа из Bellcore... это говорит о том, что он не несёт ответственности», — заявил Годвин.

Bellcore и 2600 спорят о публикации статьи 27 июля 1992 г.

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

MIDDLE ISLAND, NY — Эрик Корли, известный под псевдонимом «Emmanuel Goldstein», редактор и издатель журнала 2600 Magazine: The Hacker Quarterly, заявил Newsbytes, что угрозы со стороны Bellcore не заставят его отказаться от публикации материалов, которые он считает важными для своих читателей.

В начале этого месяца Корли получил письмо (адресованное «Emanuel Golstein») от Леонарда Чарлза Сучиты, главного юрисконсульта по вопросам интеллектуальной собственности компании Bellcore, в котором тот выразил претензии к публикации 2600 материалов, охарактеризованных им как «фрагменты определённых внутренних документов, являющихся собственностью Bellcore».

В письме далее говорилось: «Настоящим письмом мы официально уведомляем вас о том, что если в будущем вы (или ваш журнал) получите, опубликуете или иным образом раскроете какую-либо информацию или документацию Bellcore, которая (i) даёт вам основания полагать, что она является собственностью Bellcore или не была сделана ею общедоступной, либо (ii) имеет пометку "proprietary", "confidential", "restricted" или любую иную пометку, указывающую на права собственности Bellcore, — Bellcore будет настойчиво добиваться всех доступных ей правовых мер, включая, помимо прочего, судебный запрет и возмещение денежного ущерба, в отношении вас,

вашего журнала и его источников».

Хотя в письме не упоминались конкретные материалы, опубликованные 2600, Корли сообщил Newsbytes, что, по его мнению, письмо Сучиты относится к статье «U.S. Phone Companies Face Built-In Privacy Hole», опубликованной на странице 42 зимнего выпуска 1991 года. Корли пояснил: «То, что мы опубликовали, было основано на внутреннем меморандуме Bellcore 1991 года и документах Bell Operating Company, которые попали к нам через утечку. Мы не публиковали сами документы. Однако мы прочли то, что нам прислали, и написали статью на основе этого. Материал посвящён тому, как телефонные компании обеспокоены "существенной и изощрённой уязвимостью", которая может позволить использовать BLV (busy line verification — проверку занятой линии) для прослушивания телефонных переговоров».

Статья объёмом в 650 слов говорила, в частности: «Используя данную уязвимость, можно дистанционно прослушивать телефонные переговоры по выбранному номеру. Хотя телефонные компании могут делать это в любое время, недавно обнаруженная функция мониторинга в режиме самообслуживания спровоцировала своего рода кризис в телекоммуникационной отрасли».

Далее в статье объяснялось, как злоумышленники могут использовать эту уязвимость:

«Взломщик может прослушивать телефонные звонки, следуя четырём шагам:

"1. Запросить коммутатор, чтобы определить код класса маршрутизации (Routing Class Code), назначенный группе магистральных линий BLV.
"2. Найти незанятый телефонный номер, обслуживаемый этим коммутатором.
"3. С помощью недавнего изменения присвоить Routing Class Code магистральных линий BLV значению Chart Column для DN (directory number — справочного номера) незанятого телефонного номера.
"4. Добавить переадресацию вызовов на незанятый телефонный номер (Remote Call Forwarding позволило бы дистанционно задать целевой номер, тогда как Call Forwarding Fixed позволяет указывать только один целевой номер на каждое сообщение об изменении или незанятую линию)."»

«Позвонив на незанятый номер, взломщик будет направлен в группу магистральных линий BLV и подключён через "no-test vertical" к целевой телефонной линии в режиме параллельного подключения».

В статье также отмечалось: «По словам одного из документов, нет доказательств того, что хакерскому сообществу известно об этой уязвимости. Авторы выразили серьёзную обеспокоенность в связи с публикацией статьи "Central Office Operations - The End Office Environment" в электронном информационном бюллетене Legion of Doom/Hackers Technical Journal. В этой статье упоминается "No Test Trunk"».

В заключение статья констатировала: «Даже если хакерам будет закрыт доступ к этой "функции", сети BLV по-прежнему сохранят возможность использоваться для мониторинга телефонных линий. Кто будет отслеживаться и кто будет слушать — два вопроса, которые останутся без ответа навсегда».

Корли ответил на письмо Сучиты 20 июля, заявив: «Полагаю, что вы имеете в виду наше разоблачение встроенных дыр в конфиденциальности телефонной инфраструктуры, которое появилось на странице 42. В этой статье мы цитировали внутренний меморандум Bellcore, а также документы Bell Operating Company. Это не первый раз, когда мы это делаем. И не последний.

«Мы понимаем, что для вас должно быть неприятно, когда такой журнал, как наш, публикует потенциально компрометирующую информацию подобного рода. Но как журналисты мы несём определённое обязательство, которое нельзя отбросить каждый раз, когда какая-то крупная и влиятельная организация бывает раздражена. Это обязательство побуждает нас сообщать факты нашим читателям, которые живо интересуются данной темой. Если, как это нередко бывает, к нам

попадают документы, меморандумы и/или отдельные сведения в иных формах, мы имеем полное право сообщать об их содержании. Если вы видите изъян в этой логике, ваши претензии адресованы не нам, а самой концепции свободной прессы.

«И как юрист, специализирующийся на праве интеллектуальной собственности, вы знаете, что нельзя добросовестно утверждать, будто простое проставление штампа "proprietary" или "secret" на документе автоматически делает его коммерческой тайной или конфиденциальной информацией. В отсутствие конкретных пояснений, опровергающих обратное, мы вынуждены считать, что информация об общественно значимой телефонной системе и инфраструктуре представляет публичный интерес, и что Bellcore едва ли сможет доказать в суде, что какая-либо информация в нашем журнале может принести пользу конкурентам Bellcore — если, конечно, таковые у неё вообще имеются.

«Если вы всё же решите оспорить наше конституционное право на распространение важной информации о телефонной инфраструктуре, мы будем вынуждены ответить, прибегнув ко всем доступным нам правовым средствам, включая санкции, предусмотренные федеральным и государственным законодательством, а также нормами гражданского судопроизводства. Кроме того, мы будем вынуждены предать огласке ваше использование судебных исков и угроз правовых действий в целях запугивания и давления.

С уважением,
Emmanuel Goldstein»

Корли сообщил Newsbytes: «Bellcore никогда бы не осмелилась на такое в отношении New York Times. Они думают, что нас легко заставить замолчать с помощью простых угроз из-за нашего небольшого размера. Они ошибаются. Мы — ответственные журналисты; мы знаем правила и соблюдаем их. Кстати, я вышлю копию спорной статьи всем, кто об этом попросит. Читатели смогут сами решить, были ли нарушены какие-либо границы».

Корли, ведущий еженедельной программы «Off the Hook» на радиостанции WBAI в Нью-Йорке, рассказал, что обсуждал этот вопрос в эфире и получил единодушную поддержку от своих слушателей. Корли также сообщил Newsbytes, что, хотя предпочитает, чтобы его знали под псевдонимом (взятым из «1984» Джорджа Оруэлла), он понимает, что пресса вынуждена использовать его настоящее имя. Он добавил, что в ближайшем будущем «положит конец путанице, юридически сменив имя».

Сотрудники Bellcore были недоступны для комментариев относительно возможного ответа на письмо Корли.

Интервью с Ice Man и Maniac 22 июля 1992 г.

Автор: Joshua Quittner (New York Newsday) (стр. 83)

Ice Man и Maniac — двое хакеров-подпольщиков из Новой Англии, входящих в группу Micro Pirates, Incorporated. Они согласились дать интервью при условии, что их личности не будут раскрыты.

[Примечание редактора: Они безрассудны, соглашаясь на это, особенно в свете того, как публичные заявления и высказывания Phiber Optik в итоге будут использованы против него.]

В: Как вы определяете компьютерный хакинг?

Maniac: Хакинг — это не исследование компьютерных систем. Это скорее подрыв безопасности. Вот как я это вижу.

B: Сколько человек в вашей группе Micro Pirates Incorporated?

Ice Man: Пятнадцать или четырнадцать.

Maniac: У нас схожие интересы. Это способ убежать от реальности. Если у меня всё плохо в школе, я сажусь за доску и общаюсь с каким-нибудь парнем из Западной Германии, обмениваемся новыми кодами с их последних вылазок. Бегство. Забыть о реальном мире.

Ice Man: Это скорее хобби. Почему этим заниматься? Ну, невозможно просто взять и бросить. Я появился примерно полтора года назад, и, наверное, можно сказать, что я из тех, кто стоит на низшей ступени — в смысле знаний. Я занимаюсь всем этим... ну, не назовёшь это грязной работой... телефонными звонками. Я позвонил вам — вот такие дела.

B: Вы — «социальный инженер»?

Ice Man: Социальная инженерия... я не знаю, кто придумал этот термин. Это использование разговора для обмена информацией под ложным предлогом. Например, выдать себя за сотрудника телекоммуникационной компании, чтобы узнать больше о различных системах [телефонной сети].

B: Какой социальной инженерией вы занимались?

Maniac: Мы взломали систему, где хранятся оценки всей системы государственных школ. Это образовательный мейнфрейм в Kingsborough Community College. Но мы ничего не меняли.

Ice Man: Там есть мейнфрейм, хранящий все расписания, результаты Regents, идентификационные номера всех учеников нью-йоркских старших школ. Нужно входить под именем какой-либо школы, и пароль меняется каждую неделю.

B: Как вы получили пароль?

Ice Man: Методом грубой силы и социальной инженерией. Я занимался социальной инженерией прямо в школе. Притворялся наивным с одним из администраторов, задавая всевозможные вопросы — что это такое, где это находится и как туда попасть.

B: Готов поспорить, вы заглянули в свои оценки. Как там успехи?

Ice Man: Высокие восьмидесятые.

B: А вы могли изменить результаты Regents?

Ice Man: Наверное, мне бы это не сошло с рук, и я не стал бы говорить, что воздержался из моральных соображений. Скорее скажу — из соображений безопасности.

B: Какой ещё вид социальной инженерии существует?

Maniac: Есть мошенничество с кредитными картами и с телефонными картами. Звонишь и говоришь: «Я из AT&T Corporation. У нас проблема с вашей карточкой. Не могли бы вы продиктовать нам ваш четырёхзначный PIN-код?» Люди, которые в каком-то смысле богобоязненны — а AT&T для них нечто вроде бога, — говорят: «Пожалуйста, вот мой четырёхзначный PIN».

B: Хакеры из другой группы, MOD, были недавно арестованы и обвинены, в частности, в продаже инсайдерской информации о том, как проникнуть в кредитные бюро. Вы навели порядок в своих делах?

Maniac: Мы теперь понимаем, чем это грозит. Нас это уже не так привлекает. Мы понимаем, что переживают люди, когда обнаруживают, что на их кредитную карту списаны несколько тысяч долларов.

B: Вы взламывали кредитные бюро?

Ice Man: Мы собирались поискать ваше имя.

Maniac: CBI [Credit Bureau International, принадлежащий Equifax, одному из крупнейших национальных кредитных бюро] — довольно незащищённая система, если честно.

В: Вы также занимаетесь пиратством программного обеспечения?

Maniac: Изначально. Давным-давно.

Ice Man: А потом мы разветвились и перешли в сферу хакинга. Пиратство программного обеспечения — самое большое дело в компьютерном подполье. Есть такие группы, как THG и INC — они международные. THG — это The Humble Guys. INC — International Network of Crackers, и я недавно узнал, что ею руководят 14- и 15-летние. У них есть люди, работающие в компаниях, которые берут программное обеспечение, взламывают его — систему защиты — и распространяют.

В: Много ли хакерских групп в Нью-Йорке?

Maniac: Три или четыре. LOD [Legion of Doom, названный хакером Lex Luthor], MOD, MPI и MOB [Men of Business].

В: Как ваши участники общаются между собой?

Ice Man: Предпочтительный способ общения — однозначно модем [для доступа к подпольным электронным доскам объявлений, где участники оставляют сообщения друг другу или «болтают» в реальном времени]. За ним — голосовой почтовый ящик (VMB). VMB используются для связи между группами.

Компания, обычно та же, что предоставляет услуги пейджеров и автоответчиков, имеет службу голосовой почты. Звонишь [взломав код доступа, дающий возможность создавать новые голосовые ящики в системе] и вводишь номер VMB. Иногда у них есть функция исходящего дозвона, позволяющая звонить куда угодно в мире. Я каждый день звоню примерно в пять таких ящиков. На самом деле это не совсем моё.

В: Ваша группа интегрирована в расовом отношении?

Ice Man: Половина из них — азиаты. Ещё есть, кажется, один испаноязычный. Я никогда с ним не встречался. Раса, религия — никому нет дела. Единственное, что может тебя отторгнуть, — это если ты слывёшь «лузером». Если ты только берёшь, берёшь, берёшь и ничего не даёшь подполью. Важно то, насколько ты хорош и насколько тебя уважают.

Maniac: Мы не работаем по расовому или этническому принципу. Мы работаем по деловому принципу. Это организованное хобби. Ты делаешь что-то для нас и получаешь за это немного признания.

Ice Man: Точно. Если ты член нашей группы и тебе нужен высокоскоростной модем — мы дадим тебе его в пользование.

В: Как стать членом MPI?

Maniac: Нужно связаться с кем-нибудь из нас на досках.

Ice Man: И я разберусь с ними [целиком], проверю, задам вопросы, чтобы убедиться, что они знают, о чём говорят. Если всё нормально — впустим. У нас есть члены в зонах 516, 718, 212, 201, 408 и 908. Мы общаемся с кем-то из Флориды, но он ещё не участник.

В: Есть ли члены MPI, состоящие также в других хакерских группах?

Ice Man: Мне не известно ни об одном члене MPI, который был бы в другой группе. Я бы не назвал это предательством, но это как быть в двух тайных клубах одновременно. Я хочу, чтобы они были верны моей группе, а не какой-либо другой. Есть такое явление, как слияние — объединение двух групп, которое делает их больше и сильнее. Многие пиратские группы так и делали.

В: Вас не беспокоит нарушение закона?

Maniac: Нарушение закона? Меня ещё не поймали. Если поймают, я не буду глупо говорить, что просто исследовал — я не исследую. Я, в общем-то, просто навещаю. Если тебя поймают — придётся отбывать срок. Я не собираюсь с этим бороться.

Отдел ФБР помогает откусить кусок у компьютерной преступности
15 июля 1992 г.

Автор: Bill Gertz (The Washington Times) (стр. A4)

Борцы с преступностью из ФБР берут на прицел неуловимых компьютерных преступников, разъезжающих по миру с помощью клавиатуры, телефона и экрана монитора и использующих такие псевдонимы, как «Phiber Optik», «Masters of Disaster», «Acid Phreak» и «Scorpion».

«Правоохранительные органы на всех уровнях признают, что это серьёзная, нарастающая проблема преступности, и она будет продолжать расти в будущем», — заявил Чарлз Л. Оуэнс, руководитель отдела экономических преступлений ФБР.

На прошлой неделе в Нью-Йорке федеральные власти рассекретили обвинительное заключение в отношении пяти компьютерных хакеров в возрасте от 18 до 22 лет, которым предъявлены обвинения в краже услуг дальней связи и информации кредитных бюро, а также во взломе широкого спектра компьютерных сетей.

ФБР сосредотачивает своё расследование на крупных вторжениях в банковские и правительственные компьютеры, а также на случаях, когда целью является кража денег, — рассказал Оуэнс в интервью.

По его словам, количество расследований ФБР по делам о компьютерных преступлениях за последний год удвоилось; при этом жертвы сообщают о компьютерных преступлениях правоохранительным органам лишь в 11–15% случаев. Нередко пострадавшие не хотят заявлять о произошедшем из деловых или личных соображений.

В настоящее время агенты ФБР ведут более 120 дел, в том числе как минимум одно, связанное с иностранной разведкой. Половина активных дел, по словам Оуэнса, касается хакеров, действующих за рубежом, хотя подробностей он раскрывать отказался.

ФБР создало специальное подразделение из восьми человек в своём вашингтонском полевом офисе, занимающееся исключительно расследованием компьютерных преступлений.

Специальная группа, в которую входят учёные-компьютерщики, инженеры-электрики и опытные операторы компьютерных систем, первой отработала наводку, приведшую к предъявлению обвинений пятерым хакерам в Нью-Йорке, рассказал агент Джеймс К. Сеттл, возглавляющий подразделение.

Компьютерные преступники, нередко работающие на относительно примитивных компьютерах Commodore 64 или Apple II, сначала взламывают международные коммутационные телефонные сети, чтобы бесплатно звонить в любую точку мира, рассказал Сеттл.

После этого хакеры могут проводить до 16 часов в сутки, семь дней в неделю, взламывая национальные и международные компьютерные сети — такие как академический Интернет, SpanNet NASA и Milnet Пентагона.

Чтобы не быть обнаруженными, несанкционированные пользователи компьютеров «петляют и плетут маршруты» через компьютерные сети в различных местах в процессе получения информации.

«Во многом это явно продиктовано любопытством, стремлением к вызову при взломе систем, — сказал Сеттл. — Проблема в том, что они могут взять систему под контроль».

Помимо этого, добавил Оуэнс, компьютерные хакеры, похищающие информацию из коммерческих баз данных, могут обратиться к вымогательству как способу заработка.

Сеттл также отметил, что есть «признаки» вовлечения компьютерных преступников в промышленный шпионаж.

Пятеро хакеров, обвинённых в Нью-Йорке в сговоре, мошенничестве с использованием компьютеров, несанкционированном вмешательстве в работу компьютеров и мошенничестве с использованием средств связи, именовали себя «MOD» — Masters of Deception или Masters of Disaster.

В судебных документах хакеры были идентифицированы как Хулио Фернандес, 18 лет, Джон Ли, 21 год, Марк Абене, 20 лет, Элиас Ладопулос, 22 года, и Пол Стира, 22 года. Все проживают в районе Нью-Йорка.

Согласно судебным документам, Фернандес и Ли перехватывали сообщения в компьютерной сети Bank of America.

Они также взломали компьютерную сеть Martin Marietta Electronics Information and Missile Group.

Хакеры получили персональную информацию из компьютеров кредитных бюро с намерением изменить её, «чтобы сломать жизнь людей или сделать из них святых», говорится в обвинительном заключении.

И сегодняшний пароль... 26 мая 1992 г.

Автор: Robert Matthews (The Daily Telegraph) (стр. 26)

«Как не пустить упорного хакера»

Одна из любимых историй покойного физика-нобелевского лауреата Ричарда Фейнмана — о том, как он вскрыл секретные файлы с материалами по атомной бомбе в Лос-Аламосе, угадав, что комбинация замка — 271828, первые шесть цифр математической константы «е». Помимо того что это забавно, анекдот Фейнмана служит предупреждением для всех, кто использует даты, имена или распространённые слова в качестве компьютерного пароля.

Как указывает профессор Питер Деннинг из Университета Джорджа Мейсона в Вирджинии в журнале American Scientist, для всего, кроме самых тривиальных секретов, такие пароли попросту недостаточно надёжны. Пароли восходят к 1960-м годам и появлению систем разделения времени, которые позволяли множеству пользователей получать доступ к файлам, хранящимся на центральном компьютере. Не прошло много времени, как сложились стандартные приёмы незаконного получения паролей: метод образованных угадываний в стиле Фейнмана, наблюдение за пользователями, вводящими пароль, или попытки использовать общие системные пароли — «guest» или «root». Главным кошмаром безопасности, однако, является кража файла паролей пользователей, который центральный компьютер использует для проверки любого введённого пароля.

К середине 1970-х годов были разработаны способы борьбы с этим. С помощью так называемых «односторонних функций» каждый пароль шифровался таким образом, что расшифровать его было невозможно. Файл паролей тогда содержал лишь кажущиеся бессмысленными символы, очевидно бесполезные для потенциального хакера. Но, как предупреждает Деннинг, даже это можно обойти,

если пароли выбраны небрежно. Вместо попыток расшифровать файл хакеры могут просто прогонять распространённые имена и даты — или даже весь английский словарь — через одностороннюю функцию, чтобы проверить, совпадает ли результат с чем-нибудь в зашифрованном файле паролей. Это отнюдь не теоретический риск: данный метод применялся в ходе печально известного дела «Project Equalizer» в 1987 году, когда поддержанные КГБ хакеры из Ганновера взломали пароли компьютеров на базе Unix в Америке.

В конечном счёте единственный способ решить проблему паролей — освободить людей от страха забыть более сложные варианты. Долгосрочное решение, по мнению Деннинга, вероятно, связано с использованием технологии смарт-карт. Один из вариантов — карточка, генерирующая разные пароли раз в минуту по формуле, основанной на показаниях внутренних часов. Пользователь входит в систему с этим паролем. Только если компьютер подтверждает, что пароль соответствует времени входа, пользователю разрешают продолжить. Ещё одна техника смарт-карт — протокол «вызов–ответ». Пользователь сначала входит в систему под своим именем, после чего компьютер «бросает ему вызов» — на экране появляется число. Введя его в смарт-карту, пользователь получает «ответное число», генерируемое по формуле, уникальной для каждой смарт-карты. Если это число совпадает с ответом, ожидаемым от смарт-карты конкретного пользователя, компьютер предоставляет доступ. Ряд компаний уже выпускает на рынок системы на основе смарт-карт, хотя эта технология пока не получила широкого распространения.

Тем временем Деннинг утверждает, что отказ от паролей на основе английских слов повысит безопасность. Он выделяет одну простую технику создания нестандартных, но легко запоминающихся слов: «пароль-фраза». Для этого нужно просто придумать бессмысленную фразу, например «Martin says Unix gives gold forever», и использовать первые буквы каждого слова для генерации пароля: MSUGGF. Такой пароль поставит хакеров в тупик, даже если файл паролей будет украден, поскольку он не фигурирует ни в каком словаре. Однако Деннинг осторожен в гарантиях. Когда-нибудь, предупреждает он, кто-нибудь может составить компьютеризированный словарь распространённых фраз. «Этот метод, вероятно, будет хорош год-два — пока кто-то, кому нравится составлять подобные словари, не возьмётся его атаковать».

«Компьютерные копы», уступающие в огневой мощи, преследуют высокотехнологичных преступников 8 июня 1992 г.

Автор: Tony Rogers (Associated Press)

БОСТОН — Схема была проста. Когда компания заказывала авиабилет по кредитной карте, турагент вводил номер карты в свой компьютер и заказывал несколько дополнительных билетов.

Дополнительные билеты накапливались, и нечистоплотный агент продавал их за тысячи долларов.

Но в конце концов вор привлёк к себе внимание, и власти обратились к Роберту Маккенне, прокурору из офиса окружного прокурора округа Саффолк. Он — один из растущего, но всё ещё уступающего по численности отряда следователей, которые преследуют высокотехнологичных злоумышленников.

После того как вор записал на счёт местной сантехнической компании билет в Японию, его арестовала полиция, которую Маккенна внедрил под видом временных офисных работников. Он был осуждён и приговорён к году лишения свободы.

Но следователи, преследующие высокотехнологичных преступников, говорят, что слишком много преступлений можно совершить с помощью компьютера или телефона, и слишком мало детективов обучены их пресекать.

«У нас ядерный взрыв, и мы мчимся со всех ног, пытаясь спастись от взрывной волны. Но она нас накроет», — сказал Чак Джонс, курирующий расследование высокотехнологичных преступлений в Департаменте юстиции Калифорнии.

Проблема, по словам следователей, в том, что компьютеры упростили совершение таких преступлений, как банковское мошенничество. Денежные переводы, которые прежде требовали подписей и оформления документов, теперь производятся нажатием кнопки.

Но подготовка высокотехнологичного борца с преступностью требует времени.

«Мало офицеров умеют расследовать это, и мало прокуроров умеют это преследовать», — сказал Джонс.

«Нужно либо взять полицейского и сделать из него эксперта в компьютерах, либо взять компьютерного эксперта и сделать из него полицейского. Я не уверен, какой подход правильный».

Среди недавних высокотехнологичных преступлений:

• Volkswagen потерял почти 260 миллионов долларов в результате инсайдерского компьютерного мошенничества с фиктивными валютными операциями.

• Бывший сотрудник страховой компании в Форт-Уэрте, штат Техас, удалил более 160 000 записей из компьютера компании.

• Банковский служащий тайно отправил компьютерный приказ компании Brinks доставить 44 килограмма золота в отдалённое место, забрал его и исчез.

И всё же у компьютерной полиции есть свои успехи.

Секретная служба пресекла схему изготовления поддельных карточек для банкоматов, которая могла принести миллионы.

А Дон Делани, компьютерный детектив полиции штата Нью-Йорк, поймал Хайме Лириано, взломавшего систему дальней связи одной компании.

Многие корпоративные телефонные системы позволяют сотрудникам звонить на номер 800, вводить персональный идентификационный номер и совершать звонки на дальние расстояния за счёт компании.

Некоторые компьютерные хакеры используют автоматические быстронабирающие устройства — так называемые «demon dialers» — для многократного набора 800-номеров и перебора четырёхзначных кодов, пока не взломают идентификационные коды. Хакеры, применявшие этот метод, похитили телефонных услуг NASA на 12 миллионов долларов.

Лириано действовал вручную: звонил на 800-номер компании Data Products в Уоллингфорде, штат Коннектикут, из своей квартиры в Нью-Йорке. За две недели он взломал код компании.

Лириано начал продавать услуги дальней связи — по 10 долларов за 20-минутный разговор куда угодно — и клиенты выстраивались в очередь прямо в его квартире.

Но Делани отследил звонки, и 10 марта он и его бойцы выжидали у квартиры Лириано. По сигналу от New York Telephone, которая прослушивала его линию, они ворвались внутрь и застали его на месте преступления.

Лириано признал себя виновным в административном правонарушении — краже услуг — и был приговорён к трём годам условно и общественным работам.

Data Products потеряла не менее 35 000 долларов. «И мы не знаем, сколько он заработал», — добавил Делани о Лириано.

Кто платит за звонки хакеров? 12 июня 1992 г.

Автор: Kent Gibbons (The Washington Times) (стр. C1)

Компания ICF International Inc. не желает платить 82 000 долларов за несанкционированные звонки хакеров, которые проникли в коммутатор компании.

AT&T утверждает, что инженерная фирма из Фэрфакса владеет телефонной системой и несёт ответственность за звонки — в основном в Пакистан.

Теперь их спор и подобные ему оказались на рассмотрении Конгресса. Председатель подкомитета Палаты представителей считает, что необходим закон, ограничивающий сумму, которую компания может быть вынуждена заплатить за мошеннические звонки, — по аналогии с защитой пользователей кредитных карт.

Эдвард Марки, демократ из Массачусетса, проводивший слушания по данной теме, заявил, что основную часть этих расходов должны взять на себя провайдеры дальней связи и местные телефонные компании.

Пострадавшие, выступавшие на слушаниях, рассказали, что не знали о незаконных звонках, пока телефонные компании не сообщили им — иногда через несколько недель после начала подозрительной активности. Но поскольку звонки проходили через частные коммутаторы, прежде чем поступить в общедоступную телефонную сеть, правила ФКК возлагают ответственность на владельцев коммутаторов.

«Это одна из постоянных дилемм, порождённых разделением AT&T», — заявил Марки. До разукрупнения системы Bell в 1984 году каждый этап звонка проходил через сеть American Telephone & Telegraph Co., и AT&T несла ответственность за мошеннические звонки.

По различным оценкам, компании теряют от 300 миллионов до более чем 2 миллиардов долларов в год из-за этой распространяющейся формы телефонного мошенничества.

Столь широкий разброс объясняется тем, что производители коммутаторов и жертвы нередко не сообщают об убытках, чтобы избежать огласки или дальнейшего мошенничества, пояснил Джеймс Спёрлок из Федеральной комиссии по связи (FCC).

Провайдеры дальней связи заявляют, что усилили мониторинг звонков клиентов для выявления нетипичных схем — например, повторных звонков в другие страны за короткое время. В апреле Sprint Corp. добавила дополнительные защитные меры: за установочный сбор в 100 долларов и ежемесячную плату в 100 долларов — ограничение ответственности по мошенничеству в размере 25 000 долларов за инцидент.

AT&T анонсировала аналогичный план в прошлом месяце.

Роберт Фокс, помощник вице-президента Sprint по вопросам безопасности, сообщил, что новые планы снизили среднюю сумму мошеннического иска с более чем 20 000 долларов ранее примерно до 2 000 долларов за первые пять месяцев нынешнего года.

Но планов Sprint и AT&T недостаточно, считает Марки.

Неприятности ICF начались в марте 1988 года. В то время часть ICF, ставшая жертвой мошенничества, была независимой программной фирмой в Роквилле под названием Chartways Technologies Inc. ICF приобрела Chartways в апреле 1991 года.

Как и в большинстве случаев мошенничества, направленного против компаний с частными телефонными системами, высокотехнологичные злоумышленники проникли в коммутатор Chartways через бесплатный номер, открытый для клиентов компании.

Вероятно, с помощью компьютера, случайным образом набирающего телефонные номера, хакеры преодолели коды безопасности и получили тон набора для совершения внешних звонков.

Хакеры воспользовались довольно распространённой функцией, которую некоторые компании предлагают иногородним сотрудникам для экономии на международных звонках. По иронии судьбы, Chartways никогда не пользовалась этой функцией, так как она была слишком сложной, рассказал Уолтер Мессик, менеджер ICF по администрированию контрактов.

31 марта представители AT&T сообщили Chartways, что недавно было сделано 757 звонков в Пакистан на сумму 42 935 долларов.

Счёт за телефон поступил в тот же день и показал, что звонки в Пакистан начались за 11 дней до этого, рассказал Мессик.

Из-за пасхальных праздников и мониторинга звонков агентами Секретной службы функция внешних звонков ICF была отключена лишь 4 апреля. К тому времени ICF накопила почти 82 000 долларов несанкционированных звонков.

Год назад Бюро общих перевозчиков ФКК отклонило просьбу ICF списать задолженность. Полная комиссия рассмотрит апелляцию этой осенью.

Голландские хакеры считают, что закон о защите данных породит компьютерную преступность 7 июля 1992 г.

Автор: Oscar Kneppers (ComputerWorld Netherlands)

ХАРЛЕМ, Нидерланды — Голландских хакеров ждёт серьёзное наказание за взлом компьютерных систем, если в Нидерландах будет принят новый закон о компьютерных преступлениях.

Недавно обсуждавшийся в голландском парламенте и разрабатывавшийся более двух лет законопроект квалифицирует хакинг как «преступление против собственности». Ожидается, что он будет официально принят не ранее следующей весны и будет состоять из следующих трёх частей:

• Максимальное наказание для хакеров, взломавших защищённую компьютерную систему, — шесть месяцев лишения свободы.

• В случае изменения данных в системе им может грозить до четырёх лет заключения.

• Лица, незаконно получившие доступ к компьютерной системе, обслуживающей «общественные нужды», — например, больницы или муниципальные базы данных населения, — могут быть приговорены к шести годам лишения свободы.

Данный законопроект не проводит различий между компьютерными преступлениями, совершёнными внутри или вне офиса. Например, взлом пароля коллеги может повлечь уголовное преследование.

Хакеры считают, что этот закон лишь спровоцирует компьютерную преступность, поскольку они сами больше не будут предлагать «дешёвые предупреждения» компьютерным системам с плохой защитой.

Роп Гонгрийп, которого иногда называют королём голландского хакинга и который в настоящее время является главным редактором голландского журнала хакеров «Hack-tic», предупреждает, что этот закон может дать неожиданные и нежелательные результаты.

«Студенты, которые сейчас просто смотрят, что есть в системах, не зная, что это [занятие] незаконно, могут внезапно оказаться за решёткой», — сказал он. Гонгрийп сравнивает хакинг с

большой вечеринкой, куда ты заходишь без приглашения.

Гонгрийп обеспокоен последствиями нового закона для действующих хакеров. По его мнению, нынешние отношения между компьютерными хакерами и системными администраторами компаний складываются благоприятно. «[Хакеры] взламывают, например, систему электронной почты, чтобы сообщить системному администратору, что тот должен что-то сделать с безопасностью. Если этот закон будет введён, они будут осторожнее с такими [действиями]. Дешёвых предупреждений об уязвимостях в системе, следовательно, больше не будет, и вы увеличиваете шансы для так называемых настоящих преступников с сомнительными намерениями», — добавил он.

По словам представителя Министерства юстиции в Гааге, закон даёт голландской полиции и судебной системе правовой рычаг в отношении хакеров, которого им сейчас не хватает.

«Компьютерных преступников [сейчас] приходится преследовать с помощью тонких юридических трюков и обходных путей. [Раньше] требовалось немало юридической изобретательности. Но когда этот закон будет введён, арестовывать хакеров будет значительно проще», — сказал он.

Центральная криминальная разведывательная служба Нидерландов (Centrale Recherche Informatiedienst, CRI) в Гааге согласилась с этим. Эрнст Мускес, пресс-секретарь CRI, заявил: «Отрадно видеть, что теперь мы можем бороться с компьютерными преступлениями целенаправленно».

Краткие заметки PWN

1. Типограф избегает тюрьмы на первом процессе по борьбе с хакингом (Melvyn Howe, Press Association Newsfile, 9 июня 1992 г.) — Типограф-фрилансер избежал тюремного заключения на первом в Великобритании процессе по законодательству о борьбе с хакингом. Внештатный наборщик Ричард Гоулден помог разорить своих работодателей с помощью пиратской компьютерной программы — по его словам, потому что они были должны ему £2 275 задолженности по зарплате. Гоулден, 35 лет, из Колхам-Авеню, Юислей, Западный Лондон, был условно освобождён на два года после изменения своего признания с «не виновен» на «виновен» на второй день слушания в Саутуокском уголовном суде. Ему было предписано уплатить £1 200 в счёт судебных издержек и £1 250 в качестве компенсации ликвидаторам компании. Гоулден первоначально отрицал обвинение в несанкционированном изменении компьютерных данных по Закону о компьютерных злоупотреблениях 1990 года. После изменения признания судья Джон Хантер сказал ему: «Мне кажется, на самом раннем этапе этого разбирательства было очевидно, что вам нечем возразить на это обвинение». Г-н Уорвик Маккиннон, обвинитель, сообщил присяжным, что Гоулден добавил в компьютер компании Ampersand Typesetters в Кэмдене (северо-западный Лондон) программу, которая в июне прошлого года заблокировала извлечение информации без специального пароля. Три месяца спустя компания «прекратила деятельность». Г-н Джонатан Зейтлер, защитник, сказал, что Гоулден изменил признание, осознав, что непреднамеренно нарушил закон.

---

2. ICL и GM Hughes создают совместное предприятие для борьбы с компьютерными хакерами (Extel Examiner, 15 июня 1992 г.) — Подразделение General Motors Corporation — Hughes STX — и ICL создали совместное предприятие, предлагающее способы борьбы с компьютерными хакерами. Hughes STX является частью дочерней компании GM — GM Hughes Electronics Corporation. ICL на 80% принадлежит Fujitsu. По данным отраслевых источников, оборот предприятия может достичь 100 миллионов долларов в год в течение четырёх лет.

---

3. Ещё одно обвинительное заключение по делу Корнелла (Ithaca Journal, 17 июня 1992 г.) — Марк Пилгрим, Дэвид Блюменталь и Рэндалл Суонсон — все студенты Корнелла — каждый обвинён в 4 эпизодах уголовного вмешательства в работу компьютеров первой степени, 1 эпизоде вмешательства второй степени и 7 эпизодах покушения на вмешательство в работу компьютеров второй степени — в связи с распространением вируса MBDF в Интернете и на различных BBS.

Дэвид Блюменталь также обвинён в двух эпизодах подделки документов второй степени и двух эпизодах фальсификации деловых записей первой степени в связи с несанкционированным созданием учётных записей в системе VAX5 Корнелла. Ему также предъявлено ещё одно обвинение в уголовном вмешательстве в работу компьютеров второй степени в связи с инцидентом, произошедшим в декабре 1991 года.

---

4. Компьютерные сторожевые псы выводят следователей на хакера (PR Newswire, 17 июля 1992 г.) — Олимпия, Вашингтон — В четверг вечером, 16 июля, детективы Дорожной полиции штата выполнили обыск по ордеру в одном из домов в восточной Олимпии и изъяли персональный компьютер, программы и записи, сообщила Дорожная полиция штата Вашингтон.

Жилец, которого не было на месте в момент обыска, подозревается в попытках взломать компьютерные файлы Департамента лицензирования и офиса Государственного страхового комиссара.

Попытки «хакера» привели в действие компьютеризированные устройства безопасности, которые предупредили официальных лиц о попытке получить доступ по телефонному модему. Детективы патрульной службы и компьютерный персонал наблюдали за неоднократными попытками подозреваемого на протяжении нескольких недель до вручения ордера.

Для срабатывания тревоги безопасности оказалось достаточно звонка с нераспознанного компьютера. Внутренняя система безопасности затем сохранила все попытки ввода данных со стороны несанкционированного пользователя для последующего извлечения и использования правоохранительными органами. Целостность государственных систем нарушена не была.

Расследование продолжается с целью установить, могут ли несколько знакомых подозреваемого быть причастны к взлому. Ожидается, что обвинения будут предъявлены уже на следующей неделе.

КОНТАКТ: Сержант Рон Напп из Дорожной полиции штата Вашингтон, (206)459-6413

---

5. По данным UPI, телефонный код 313 будет разделён на новый код 810 с 10 августа 1994 года.

Округа Окленд, Маком, Дженеси, Лапир, Сент-Клэр и Санилак, а также небольшие части округов Сагино, Шиауасси и Ливингстон перейдут в зону 810. Округа Уэйн, Вошто, Монро, а также небольшие части округов Джэксон и Ленауи останутся в зоне 313. Город Детройт находится в округе Уэйн и не изменится.