твоя жизнь, свобода и благополучие в эпоху цифрового нашествия

АТАКА БИТОВ

Хэл Абельсон
Кен Ледин
Гарри Льюис

Цифровая экспансия изменяет мир сильнее, чем кажется

Символ®

По договору между издательством «Символ-Плюс» и Интернет-магазином «Books.Ru – Книги России» единственный легальный способ получения данного файла с книгой ISBN 978-5-93286-162-2, название «Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху» – покупка в Интернет-магазине «Books.Ru – Книги России». Если Вы получили данный файл каким-либо другим образом, Вы нарушили международное законодательство и законодательство Российской Федерации об охране авторского права. Вам необходимо удалить данный файл, а также сообщить издательству «Символ-Плюс» (piracy@symbol.ru), где именно Вы получили данный файл.

Blown to Bits

Your Life, Liberty, and Happiness after the Digital Explosion

Hal Abelson, Ken Ledeen, Harry Lewis

Addison-Wesley

Атака битов

Твоя жизнь, свобода и благополучие в цифровую эпоху

Хэл Абельсон, Кен Ледин, Гарри Льюис

Санкт-Петербург — Москва
2009

Хэл Абельсон, Кен Ледин, Гарри Льюис

Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху

Перевод А. Балаева

Главный редактор	*А. Галунов*
Зав. редакцией	*Н. Макарова*
Выпускающий редактор	*П. Щеголев*
Редактор	*Т. Темкина*
Корректор	*С. Минин*
Верстка	*К. Чубаров*

Абельсон Х., Ледин К., Льюис Г.

Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху. – Пер. с англ. – СПб.: Символ-Плюс, 2009. – 392 с., ил.

ISBN 978-5-93286-162-2

Ежедневно миллиарды фотографий, музыкальных файлов, новостных статей и сообщений электронной почты разносятся по всему миру потоками битов. Цифровые технологии породили небывалые возможности для нововведений, сотрудничества, развлечений и демократического управления обществом. И они же все больше подтачивают вековые представления об индивидуальности, свободе слова и праве на частную жизнь.

Можете ли вы контролировать тех, кто собирает о вас информацию? Считаете ли вы, что электронная почта может быть конфиденциальной в условиях, когда ничто не кажется защищенным от чужих глаз? Следует ли подвергнуть Интернет такой же цензуре, как радио и телевидение? Является ли скачивание музыки преступлением? Как на самом деле поисковики, вроде Google или Yahoo!, определяют, какие сайты вам показать? Сохраняется ли в цифровом мире ваше право на свободу слова? Имеет ли значение ваше мнение при разработке правительственной или корпоративной политики конфиденциальности?

Здесь вы найдете провокационные ответы на эти вопросы и впечатляющие истории из реальной жизни. Книга призывает человечество осознать происходящее и начать противостоять цифровой экспансии.

ISBN 978-5-93286-162-2
ISBN 978-0-13-713559-2 (англ)

© Издательство Символ-Плюс, 2009
Authorized translation of the English edition © 2008 Pearson Education, Inc. This translation is published and sold by permission of Pearson Education, Inc., the owner of all rights to publish and sell the same.

Все права на данное издание защищены Законодательством РФ, включая право на полное или частичное воспроизведение в любой форме. Все товарные знаки или зарегистрированные товарные знаки, упоминаемые в настоящем издании, являются собственностью соответствующих фирм.

Издательство «Символ-Плюс». 199034, Санкт-Петербург, 16 линия, 7,
тел. (812) 324-5353, www.symbol.ru. Лицензия ЛП N 000054 от 25.12.98.
Налоговая льгота – общероссийский классификатор продукции
ОК 005-93, том 2; 953000 – книги и брошюры.

Подписано в печать 30.07.2009. Формат 70×100 1/16. Печать офсетная.
Объем 24,5 печ. л. Тираж 1500 экз. Заказ №
Отпечатано с готовых диапозитивов в ГУП «Типография «Наука»
199034, Санкт-Петербург, 9 линия, 12.

Посвящается нашим детям: Аманде,
Дженнифер, Джошуа, Илии, Энни и Элизабет,
которым еще предстоит увидеть,
как мир в очередной раз непредсказуемо изменится.

Оглавление

Об авторах 12

Отзывы о книге 13

Предисловие 15

Благодарности 16

Глава 1 | Цифровая экспансия 17

Битовый взрыв и окружающий мир 18
Коаны о битах 21
Коан первый: все это – только биты 22
Коан второй: совершенство – это естественное состояние 24
Коан третий: изобилие порождает нищету 24
Коан четвертый: вычисления – сила 25
Коан пятый: количество переходит в качество 27
Коан шестой: ничто не исчезает бесследно 29
Коан седьмой: биты движутся быстрее мысли 30
Добро и зло, перспективы и риски 32
Сами по себе технологии ни хороши, ни плохи 32
Новые технологии несут в себе как риски, так и перспективы 34

Глава 2 | Под всевидящим электронным оком 37

1984 – реальность, но мы рады 37
Следы ног и отпечатки пальцев 41
Улыбайтесь, мы вас снимаем! 41
Ваши перемещения отслеживаются 43
Ваша обувь расскажет о своих путешествиях 44
«Черные ящики» есть не только в самолетах 47
Следы на бумаге 49
Автостоянка знает больше, чем вы думаете 50
Вся информация в одном кармане 51
Собирая мозаику 52
Почему мы утратили (или просто отбросили) право на неприкосновенность частной жизни 57

Экономия времени 58
Экономия денег 59
Ради удобства покупателей 61
Разоблачаться – это просто забавно 62
Потому что иначе никак 63
Младший Брат смотрит на тебя 64
Публичные документы становятся общедоступными 64
Праздное любопытство 68
«Старший Брат» в США и везде 70
«Говорите, мы вас слушаем!» 71
Идентификация граждан: нет ID-картам! 72
Плодотворное сотрудничество «Старших Родственников» 73
Смена технологий – смена стиля жизни 78
Культура кредитных карт 79
Культура электронной почты 79
Веб-культура 81
За границами частной жизни 84
Оставьте меня в покое 84
Неприкосновенность частной жизни и свобода 86
Принципы добросовестного использования информации 88
Право на неприкосновенность частной жизни как право контролировать информацию 93
Включены постоянно 96

Глава 3 | Фантасмагории электронного мозга 98

Компьютер знает о вас намного больше, чем показывает 98
Внося исправления, не забывайте о том, что они сохраняются ... 102
Служебная информация, сохраняемая в электронном документе 104
Можно ли препятствовать утечке информации? 106
Представление, реальность и иллюзия 107
Что есть правильное представление 111
Снижение количества данных (в том числе без потери информации) 115
Рождение и гибель технологий 117
Форматы данных как общественная собственность 118
Изображения скрывают информацию 122
Война со спамом 122
Скрытие информации от неискушенного наблюдателя 124
Пугающие секреты старых дисков 126
Что происходит с данными при удалении файла? 129
Можно ли стирать данные необратимо? 132
Сколько в действительности «живут» данные? 133

Глава 4 | Иголки в стоге сена ... 137

Найдены спустя семьдесят лет ... 137
Библиотека и базар ... 138
До запретного плода – всего один щелчок ... 142
Крушение иерархии ... 146
Как это работает ... 149
Шаг 1: сбор информации ... 151
Шаг 2: сохранение копий ... 154
Шаг 3: формирование индекса ... 156
Шаг 4: разбор текста запроса ... 158
Шаг 5: определение адекватности каждого из полученных результатов ... 160
Шаг 6: определение приоритетности полученных результатов (ранжирование) ... 163
Шаг 7: представление результатов ... 168
Кто и за что платит? ... 170
Некоммерческий поисковый сервис ... 171
Размещения, переходы и аукционы ... 172
Дядя Сэм делает заметки ... 174
Сервис Google находит решение без компромиссов ... 175
Запрещенная реклама ... 176
Поиск – сила ... 177
Выполнение по алгоритму не означает отсутствие ошибок ... 178
Поисковые системы не одинаковы ... 179
Выводом результатов поиска можно управлять ... 181
Поисковые системы не могут видеть всего ... 185
Контроль поиска и контроль умов ... 185
ЧТО вы искали? Отслеживание поисковых запросов ... 190
Контроль и замена посредников ... 192

Глава 5 | Засекреченные биты ... 196

Средства шифрования в руках террористов и прочих ... 196
Почему бы не контролировать шифрование? ... 198
История криптографии ... 201
Взлом шифров замены ... 202
Секретные ключи и одноразовые шифры ... 205
Уроки для эпохи Интернета ... 210
Прорывы случаются, но вести доходят медленно ... 210
Доверять хорошо, но лучше знать ... 211
Мало иметь надежную систему – нужно ее использовать ... 212
Противник знает вашу систему ... 213
Открытие, навсегда изменившее криптологию ... 215

Протокол соглашения о ключе 218
Открытые ключи для закрытых сообщений 220
Цифровые подписи 220
Стандарт шифрования RSA 222
Цифровые сертификаты и центры сертификации 223
Шифрование для всех 224
Настоящее и будущее шифрования 229

Глава 6 | Нарушение равновесия 232

Автоматизированное правосудие для автоматизированных преступлений 232
26 000 исков за 5 лет 233
Правонарушение вам дорого обойдется 235
Акт о противодействии электронному воровству: распространение цифровых копий –это преступление 237
Технологический переворот: peer-to-peer 240
Наказание за соучастие 241
Файловый обмен становится децентрализованным 244
Правовая защищенность не гарантируется 246
Вопрос намерения 248
Использовать только с разрешения 251
Цифровые права и доверенные системы 252
Контроль за пределами защиты авторских прав 255
Запрещенная технология 257
Защита авторских прав или боязнь конкуренции? 260
Лицо монополизированной технологии 262
«Коянискацци» защиты от копирования: жизнь, выведенная из равновесия 264
Опоздавшая ставка 267
Движение к перемирию 269
Пределы собственности 273
Учимся летать в цифровых облаках 274

Глава 7 | О чем нельзя говорить в Интернете 278

Знаете ли вы, какие сайты посещал сегодня ваш ребенок? 278
Как назвать то, не знаю что? 281
Издатель или распространитель? 284
Ни свободы, ни безопасности 286
Самое отвратительное место на Земле 287
Самая демократичная форма массового общения 289
Защита добрых самаритян... и некоторых злых 293
Законы с непредусмотренными последствиями 297
Можно ли считать Интернет журнальным киоском? 299

Преследование с помощью клавиатуры 302
Всего лишь досаждающий телефонный звонок? 304
Цифровая защита, цифровая цензура и самоцензура 306

Глава 8 | Биты в эфире 312

Цензура для президента 312
Как регулируется эфир 314
От беспроводного телеграфа к беспроводному хаосу 316
Радиоволны на выделенных каналах 319
Национализация полосы частот 323
Козлиные тестикулы и Первая поправка 324
Переход к отказу от регулирования диапазона 328
От нескольких труб к миллионам флейт 329
Можно ли просто поделить диапазон на всех? 331
Совместное использование диапазона 333
Самый красивый изобретатель в мире 334
Емкость канала 337
Мощность, сигнал, помехи и полоса пропускания 339
Для одного сигнал, для другого помеха 341
Радиодиапазон для всеобщего пользования 343
Что ждет радиосвязь в будущем? 347
Если бы радиоустройства были интеллектуальными 347
Нужна ли нам цифровая экспансия? 350
Какой объем государственного контроля необходим? 352

Заключение | После взрыва 355

Биты, освещающие весь мир 355
Пара битов напоследок 359

Приложение | Интернет как система и образ мышления 361

Интернет как система связи 361
Коммутация пакетов 361
Ядро и периферия 363
IP-адресация 363
Ключ ко всему: передача пакетов 366
Протоколы 367
Надежность Интернета 369
Интернет как образ мышления 370
Песочные часы 370
Уровни, а не башни 373
Сквозное соединение 374
Отделение содержимого от среды передачи данных 375
Открытые интерфейсы 377

Об авторах

Хэл Абельсон (Hal Abelson) – преподаватель электротехники и информатики Массачусетского технологического института (Massachusetts Institute of Technology, MIT) и пожизненный член Института инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronics Engineers, IEEE). Он способствовал внедрению инновационных технологий обучения, таких как OpenCourseWare, участвовал в основании Creative Commons и Public Knowledge, а также был основателем и директором Фонда свободного программного обеспечения (Free Software Foundation, FSF).

Кен Ледин (Ken Ledeen) – президент и исполнительный директор компании Nevo Technologies, обслуживающей интегрированные системы многих технологических компаний.

Гарри Льюис (Harry Lewis) – бывший декан Гарвардского колледжа, профессор компьютерных наук Гарвардского университета (стипендиат фонда Гордона Маккея), стипендиат Центра Беркмана изучения Интернета и общества, автор книги «Excellence Without a Soul: Does Liberal Education Have a Future?» (Бездушное превосходство: есть ли будущее у либерального образования?).

Авторы совместно ведут в Гарварде курс математических методов управления (Quantitative Reasoning 48) – новейший курс для студентов гуманитарных специальностей.

Отзывы о книге

Про цифровой мир пишут, в основном, либо технари, описывая технические моменты для других технарей, либо ученые мужи, глубокомысленные речи которых далеки от их технических познаний. В этой книге эксперты по информационным технологиям напрямую отсылают читателей к реальным фактам и закономерностям, к которым мы все питаем живой интерес.

Говард Гарднер, профессор Высшей педагогической школы Гарвардского университета, исследователь закономерностей познания и обучения, автор книги «Multiple Intelligences and Changing Minds»

Независимо от ваших знаний о компьютерах книга покажет вам исключительно интересные и познавательные перспективы, открытые величайшими умами цифровой индустрии.

Эта увлекательная, глубокая и поучительная книга поможет вам совершенно по-новому оценить сущность компьютеров и их влияние на мир.

Это одна из тех редких книг, которые описывают последствия цифрового нашествия языком, понятным любому, одновременно призывая специалистов окинуть привычные вещи свежим взглядом.

Анна Маргулис, помощник секретаря по информационным технологиям и руководитель информационного департамента правительства штата Массачусетс

Очень остроумная и вместе с тем глубокая книга. До чего приятно видеть, как настоящие преподаватели дают студентам цифровой эпохи действительно прочную основу для понимания их цифрового окружения, его аксиом и связанного с ним законодательства, начиная с трудов Клода Шеннона. Я с нетерпением жду, когда авторы откроют курс онлайн-обучения.

Чарльз Нессон, профессор Гарвардской школы права, основатель Центра Беркмана изучения Интернета и общества

Для многих из нас компьютеры и Интернет по-прежнему являются чем-то волшебным. Мы создаем нечто, отправляем нечто, получаем нечто и покупаем нечто. Мы всего лишь перемещаем указатель мыши, щелкаем мышью, копируем и вставляем. Но сущность этих действий окутана покровом тайны. Эта книга простыми и понятными словами объясняет, как работает этот механизм, стоящий на моем столе, и почему нам следует обращать больше внимания на революционные изменения, которые подобные штуки вносят в нашу жизнь. Это блестящая книга, совершенно необходимая потребителям, рядовым гражданам и студентам всех возрастов.

Шива Вайдхьянатан, адъюнкт-профессор по исследованию рекламы и права Университета штата Вирджиния, автор книги «Copyrights and Copywrongs: The Rise of Intellectual Property and How it Threatens Creativity»

Мир – как слон из притчи, а мы – как слепцы. И стар и млад рискуют попасть под контроль технологий, вместо того чтобы самим управлять происходящим. Эта книга может стать для многих тем же, чем стал Розеттский камень для египтологов, помогая понять, как в новом, цифровом мире уживаются право, технология, культура, информация. Взорвут ли жизнь новые возможности или заставят ее пойти на уступки? Создавшееся положение и возбуждает, и подавляет. Абельсон, Ледин и Льюис вместе смогли описать слона. Читатели этой небольшой книги, посвященной начальному этапу великого путешествия человечества, смогут сделать первый шаг, получив основу для понимания и самостоятельного накопления новых фактов, которые не замедлят появиться. «Эту книгу следует прочесть» – может, звучит и банально, но в данном случае это правда.

Харви Силверглейт, писатель и адвокат по уголовным и гражданским делам

Предисловие

Тысячи лет люди замечали, что мир меняется, никогда не возвращаясь к прежнему состоянию. Коренные изменения в наше время отличаются тем, что зависят от развития соответствующих технологий. Сейчас в принципе возможно записать и сохранить все, что каждый человек скажет, напишет, споет, нарисует или сфотографирует. *Абсолютно все*. Цивилизация накопила достаточно дисков и карт памяти, чтобы хранить оцифрованный мир до тех пор, пока существуют и производятся компьютеры. Глобальные компьютерные сети моментально делают накопленное доступным всей планете. И компьютерам достанет мощи в мгновение ока извлечь из этой информации то, что соответствует заданным критериям поиска, и связать в цельную картину.

В минувшие века человек мог увидеть подобное только в мечтах (или в кошмарах). Сегодня мечты (и кошмары) становятся явью. Мы живем во времена перемен и можем наблюдать, как они происходят. Но даже мы не знаем, чем это для нас обернется.

Прямо сейчас правительства и другие общественные институты решают, как им использовать новые возможности. Все мы участвуем в обсуждениях и принятии решений, касающихся нас самих, наших семей и сотрудников. Каждый должен знать, как он сам и окружающий мир изменяются под действием нахлынувшего потока цифровых технологий. Каждый должен понимать, как принятые решения повлияют на его жизнь, на жизнь его детей, внуков и следующих поколений.

Вот почему мы написали эту книгу.

Каждый из нас больше сорока лет проработал в области информационных технологий. Книга, которую вы сейчас читаете, – результат наших наблюдений за цифровым нашествием и нашим участием в нем. Каждому из авторов в свое время приходилось быть как учителем, так и учеником. Содержание книги связано с общеобразовательным курсом, который мы ведем в Гарварде, но не думайте, что это сухой учебник. Мы постарались добавить картине ярких красок и надеемся, что размышляя, вы не будете скучать.

Главы книги можно читать в любом порядке. В приложении подробно объяснены принципы работы Интернета. Для чтения этой книги не нужен компьютер. Но мы все же предполагаем, что он у вас есть, как и подключение к Интернету. Они могут вам пригодиться, если

какая-то из тем привлечет ваше внимание. Не стесняйтесь спрашивать вашу любимую поисковую систему и изучать результаты запроса. В книге есть много ссылок на сайты с описанием их ресурсов, например *bitsbook.com* (сайт этой книги). Но, как правило, поисковые системы позволяют быстрее и проще найти то, что вас интересует. Есть множество интересных открытых источников информации и интернет-сообществ, где вы можете больше узнать и принять участие в глобальном обсуждении предмета книги.

В этой книге мы развиваем свои теории. Если вы хотите высказаться, предлагаем зайти на вышеупомянутый сайт и поучаствовать в текущем обсуждении. Мы описали картину цифрового нашествия на культуру и правовую систему США, но поднимаемые вопросы жизненно важны для любого гражданина любого свободного общества и для всех, кто стремится сделать свое общество более свободным.

Кембридж, Массачусетс.
Январь 2008 года

Благодарности

Принимая на себя полную ответственность за все ошибки в материалах этой книги, мы также должны выразить свою признательность многим людям, чья помощь способствовала более глубокому пониманию сути нашей работы. Особой благодарности заслуживают те, чьи замечания или действия помогли улучшить черновой вариант книги: Линн Абельсон (Lynn Abelson), Мэг Аусман (Meg Ausman), Скотт Браднер (Scott Bradner), Арт Бродски (Art Brodsky), Майк Кэрролл (Mike Carroll), Маркус Кон (Marcus Cohn), Фрэнк Корнелиус (Frank Cornelius), Алекс Кертис (Alex Curtis), Наташа Деврю (Natasha Devroye), Дэвид Фарентхольд (David Fahrenthold), Роберт Фэрис (Robert Faris), Иоганн-Кристоф Фрейтаг (Johann-Christoph Freytag), Венди Гордон (Wendy Gordon), Том Хемнес (Tom Hemnes), Брайан ЛаМаччиа (Brian LaMacchia), Маршалл Лернер (Marshall Lerner), Энн Льюис (Anne Lewis), Элизабет Льюис (Elizabeth Lewis), Джессика Литман (Jessica Litman), Лори Лайбек (Lory Lybeck), Фред фон Ломан (Fred von Lohmann), Мерлин Макграт (Marlyn McGrath), Майкл Маркус (Michael Marcus), Майкл Митценмахер (Michael Mitzenmacher), Стив Папа (Steve Papa), Джонатан Пирс (Jonathan Pearce), Брэдли Пелл (Bradley Pell), Лес Перельман (Les Perelman), Памела Самуэльсон (Pamela Samuelson), Джефф Шиллер (Jeff Schiller), Кэти Слудер (Katie Sluder), Джиджи Сон (Gigi Sohn), Дебора Спар (Debora Spar), Рене Штейн (Rene Stein), Алекс Тиббетс (Alex Tibbetts), Сюзанна Тобин (Susannah Tobin), Салил Вадхан (Salil Vadhan), Дэвид Уорш (David Warsh), Данни Вейтцнер (Danny Weitzner) и Мэтт Уэлш (Matt Welsh).

Глава 1 | Цифровая экспансия

С чего все началось и чем это угрожает

19 сентября 2007 года под Сиэттлом произошла авария. Автомобиль Тани Райдер, вылетев с шоссе, провалился в глубокую расселину.[1] Восемь дней женщина была зажата в искореженном автомобиле. Страдая от обезвоживания, с травмированными бедром и плечом, она могла умереть из-за отказа почки. К счастью, спасатели после длительных поисков обнаружили пострадавшую. Несколько месяцев миссис Райдер провела в клинике, но Рождество все же смогла встретить дома.

История миссис Райдер – не только о женщине, дорожной аварии и спасении. Она также о битах – нулях и единицах, из которых состоят все мобильные разговоры, банковские записи и вообще все то, что использует передачу или хранение информации средствами современной электроники.

Миссис Райдер нашли благодаря тому, что операторы сотовой связи фиксируют местоположение телефонов. Включенный сотовый телефон регулярно посылает на базовую станцию цифровой «пинг» (ping), несколько битов – сообщение типа «я здесь». Ближайшая станция, принявшая сигнал, передает его сотовому оператору. Полученные сведения нужны оператору для правильного перенаправления входящих вызовов. Компания Verizon, оператор миссис Райдер, сохранила сведения о последнем местонахождении ее мобильного телефона, хотя сам телефон при аварии «не выжил». Поэтому полиция и спасатели смогли найти пострадавшую.

Но почему это заняло больше недели?

---

[1] Дженнифер Салливан (Jennifer Sullivan) «Last phone call steered search» (Последний звонок по телефону дал ключ к поиску), *Seattle Times* от 2 октября 2007 года; Уильям Ярдли (William Yardley) «Missing woman found alive in wrecked car after 8 days» (Пропавшая женщина найдена живой в автомобиле через 8 дней после аварии), *New York Times* от 29 сентября 2007 года.

Когда исчезает женщина, ее муж не может просто пойти в полицию и потребовать отыскать ее с помощью сотового оператора. У нее есть право на неприкосновенность частной жизни и могут быть достаточно веские причины оставить город, ничего не сообщая мужу. После исчезновения Тани Райдер ее банковский счет время от времени активизировался (снова биты!), следовательно, полиция не могла признать ее «пропавшей без вести».

На самом деле счет активизировал ее муж. По какому-то недоразумению полиция не подумала о такой возможности. Только предположив, что муж миссис Райдер причастен к ее исчезновению, полиция получила законное основание для просмотра записей сотового оператора. Если бы полиция действовала на основании (верного) предположения о невиновности мужа, возможно, миссис Райдер вообще бы не нашли.

Новейшие технологии довольно своеобразно взаимодействуют с правом на неприкосновенность частной жизни, средствами коммуникации и уголовным законодательством. Получившаяся взрывоопасная смесь едва не стоила Тане Райдер жизни. Ее случай производит сильное впечатление, однако каждый день мы встречаем неожиданные и не менее впечатляющие следствия влияния потоков данных, попросту невозможные еще несколько лет назад.

Дочитав эту книгу, вы посмотрите на мир другими глазами. Услышав рассказ друга или сообщение в новостях, вы скажете себе: «Это действительно история о битах», – даже если цифровые технологии не упоминались. Перемещения неодушевленных предметов или действия живых людей из плоти и крови – только вершина айсберга. Чтобы понять, что на самом деле происходит, вам придется окунуться в виртуальный мир и самому увидеть великий и ужасный поток битов, незаметно направляющий течение жизни.

Эта книга послужит вам проводником в этот новый мир.

Битовый взрыв и окружающий мир

Мир резко изменился. Почти все хранится в компьютере. Судебные протоколы, списки покупок, любимые семейные фотографии, никчемные радиопередачи… Компьютеры хранят кучу материалов, которые сегодня не нужны, но, как кое-кто полагает, могут когда-нибудь пригодиться.

На нижнем уровне все это состоит из нулей и единиц – битов. Биты скапливаются на дисках домашних компьютеров и накопителях данных крупных корпораций и правительственных агентств. Эти накопители могут хранить так много бит, что уже нет необходимости просеивать информацию и выбирать, что ценно, а что нет.

В цифровом виде хранится так много информации и дезинформации, нужных и ненужных уже данных, что большая часть содержимого накопителей будет видна только компьютеру и никогда не попадет на глаза человеку. И компьютеры все лучше справляются с задачей выборки информации по заданным критериям. Иногда настолько успешно, что даже раскрывают преступления, дают полезные советы или выносят на всеобщее обозрение то, что мы никогда не решились бы обнародовать.

Уход Элиота Шпитцера с поста губернатора штата Нью-Йорк в марте 2008 года[1] – это очередная «история битов». В этой истории главной движущей силой явилась проституция. И эта история могла бы не произойти, если бы не вмешательство битов. В соответствии с законодательством по борьбе с отмыванием денег банки должны предоставлять федеральным управляющим отчеты по транзакциям на суммы, превышающие 10 тысяч долларов. Ни одна из инициированных губернатором операций не превысила пороговой суммы, однако банковский компьютер выявил подозрительную закономерность небольших выплат. Вообще-то меры по борьбе с отмыванием денег направлены против терроризма и организованной преступности. Но в этом случае компьютер, сканирующий транзакции в поисках следов тяжких преступлений, выявил рядовой счет об оплате услуг. Этот счет поставил точку в карьере губернатора Нью-Йорка.

То, что как-либо попало в компьютер, может быть многократно размножено и распространено по всему свету за несколько секунд. Представьте себе миллион абсолютно идентичных копий того, чем вы хотите поделиться с миром. И миллион абсолютно идентичных копий того, о чем предпочли бы не заикаться.

Цифровая экспансия изменяет мир так же, как в свое время его изменило изобретение книгопечатания. Новые веяния застают нас врасплох, в корне меняя наше мировоззрение.

Разные проявления цифрового взрыва могут казаться полезными, восхитительными или даже неосуществимыми. Вместо того чтобы отправить фотоснимки бабушке почтой, мы выкладываем фото своих детей на веб-сайте сервиса фотоальбомов, вроде Flickr. После этого фотографии может увидеть не только бабушка или ее друзья, но и кто угодно. «И что? – скажете вы. – Эти фотографии милы и безобидны!» Но предположим, что вы случайно оказались на заднем плане снимка, сделанного неким туристом в ресторане, где ваше присутствие не предполагалось. Если турист выложит эту фотографию в Сети, весь мир узнает о том, где вы были и когда.

Информация склонна просачиваться. Записи операций с кредитными карточками должны храниться в защищенных хранилищах, однако

[1] О том, как банковский компьютер вывел на чистую воду губернатора, см. *blogs.zdnet.com/BTL/?p=8211&tag=nl.e540*.

эти сведения часто попадают в руки мошенников. Иногда мы сами создаем утечку информации, получая нечто взамен. К примеру, компания[1] предоставляет возможность бесплатно позвонить в любую точку мира в обмен на просмотр рекламы. При этом компьютеры компании слышат, о чем вы говорите.

Сегодня все это в порядке вещей. Экспансия только начинается, и ее последствия – разрушение основ общества – уже не за горами.

Мы уже живем в мире, где *даже памяти цифровой камеры* достаточно для хранения текстового содержания всех книг Библиотеки Конгресса США. Интенсивность пересылки электронной почты такова, что за десять минут можно передать все собрание Библиотеки Конгресса. Оцифрованные фотографии и звукозаписи занимают больше места, чем текст, так что пересылка по электронной почте всех иллюстраций, видео- и звукозаписей может занять год – но это сегодня. Мощь битового взрыва нарастает. Каждый год мы получаем возможность хранить еще больше информации, передавать ее еще быстрее и производить с ней операции, недоступные в прошлом году.

Ежегодно производится так много устройств хранения данных[2], что их достаточно для того, чтобы каждую минуту-две записывать примерно страницу информации *о каждом жителе Земли*. Некогда сделанное замечание может сорвать предвыборную кампанию; черновик письма может стать открытием для биографа. Только представьте, что значит сохранять все, что каждый сказал или написал за целую жизнь. Технических препятствий для этого уже нет: емкости накопителей более чем достаточно. Должно ли общество сопротивляться этому?

Некоторые вещи открываются как с положительной, так и с отрицательной стороны. «Публичная запись» сегодня *воистину* публична: ваш потенциальный работодатель из Нэшвилля (штат Теннесси) может выяснить, что десять лет назад в Луббоке (штат Техас) вы были оштрафованы за левый поворот в неположенном месте. В мире, где каждая подробность многократно продублирована, занесена в каталоги и свободна для ознакомления и распространения, прежнее понятие судебной тайны обращается в миф.

В США сотни теле- и радиостанций и миллионы веб-сайтов, готовых предоставить новости на любой вкус. При таком выборе американцы

---

[1] Компания Pudding Media, *puddingmedia.com*.

[2] Латанья Суини (Latanya Sweeney) «Information Explosion» (Информационный взрыв); Л. Заяц, П. Дойл, Дж. Тьюз, Дж. Лэйн (L. Zayatz, P. Doyle, J. Theeuwes, J. Lane) «Confidentiality, Disclosure, and Data Access: Theory and Practical Applications for Statistical Agencies» (Конфиденциальность, разглашение и доступ к данным: теоретическое и практическое применение для статистических агентств), Институт экономики города, Вашингтон, округ Колумбия, 2001.

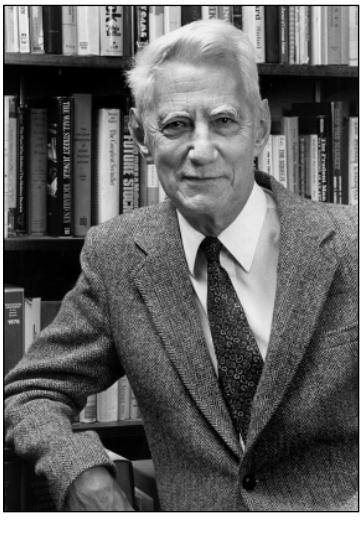
могут критически оценивать новости из официальных источников. В Китае обратная ситуация: совершенные технологии позволяют государству управлять информацией, получаемой гражданами, и контролировать их действия.

Эта книга о том, как цифровая экспансия изменяет весь мир. Она объясняет саму суть цифровых технологий: почему у них так много побочных эффектов и почему многое не работант так, как ожидалось. Эта книга о разрушительном воздействии цифровых технологий на нашу частную жизнь, нашу индивидуальность, и о том, кто контролирует наши жизни. Вы узнаете, как создавались условия для цифровой экспансии, что мы потеряли и каковы наши шансы на победу и выживание. Цифровая экспансия создает как перспективы, так и риски. Многие последствия того и другого проявятся в течение ближайших десяти лет. Правительства, корпорации, другие влиятельные структуры пользуются возникшей всеобщей неразберихой, и большинство из нас даже не замечает этого.

Нам всем есть, что терять. Будучи вне технологии, истории, права и политики, эта книга призывает вас очнуться от сна. Силы, формирующие ваше будущее, основаны на цифровых технологиях, и вы должны знать их в лицо.

Коаны о битах

Биты ведут себя странно. Они почти все время движутся и почти не занимают места. Чтобы лучше понимать их, мы применяем метафоры из физического мира. Мы сравниваем их поведение со взрывом



Клод Шеннон

Клод Шеннон (1916–2001) – один из основателей теории связи и информации. После Второй мировой войны работал в компании Bell Telephone Laboratories. В 1948 г. опубликовал монографию «Математическая теория связи», предопределившую последующее развитие цифровых технологий. В ней, в частности, определен бит как естественная единица измерения информации и изложена математическая модель идеальной системы связи.

Alcatel-Lucent, *http:www.bell-labs.com/news/2001/february/26/shannon2_lg.jpeg*

или водным потоком. Часто применяются и метафоры из общественной жизни. Мы говорим, что два компьютера соединяются для обмена битами, людей, получающих доступ к «чужим» битам, называем «взломщиками». Важно выбирать правильные аналогии; так же важно понимать ограничения выбранных аналогий. Туманная терминология может создать ложное представление, удачная может привести к озарению.

Вашему вниманию предлагаются семь битовых истин. Мы назвали их «коанами», потому что эти парадоксы подобны дзенским притчам, побуждающим к поиску истины и приводящим к просветлению. Эти коаны являются упрощениями и обобщениями. Они описывают динамично развивающийся, но мало исследованный мир. При всей своей упрощенности битовые коаны ближе к истине, чем мы обычно представляем. По мере чтения книги вам будет все легче находить подтверждения истинности битовых коанов.

Коан первый: все это – только биты

Ваш компьютер успешно создает иллюзию того, что в нем хранятся фотографии, письма, музыкальные произведения и фильмы. На самом деле компьютер хранит только нули и единицы, нужным образом оформленные и упорядоченные. Компьютер создан так, что может хранить только биты: все файлы, каталоги и данные различных типов – лишь иллюзия, созданная программистами. Когда вы отправляете по электронной почте письмо с прикрепленной фотографией, компьютеры, выполняющие пересылку, не имеют никакого представления о том, что содержимое сообщения частично является текстом, а частично изображением.

Конкуренция телефонных компаний, сотовых операторов, операторов кабельного телевидения и провайдеров IP-телефонии (VoIP) усугубляется тем, что, несмотря на все различия оказываемых ими услуг, они всего лишь пересылают с узла на узел массивы битов. Интернет был создан для транспортировки битов, а не электронной почты, изображений или каких-либо других программно-инженерных разработок. Мы находим для них интуитивные соответствия. Но если копнуть глубже, все это – только биты.

Этот коан обладает более глубоким смыслом, чем вы могли бы подумать. Взгляните на описание конфликта компаний Naral Pro-Choice America и Verizon Wireless.[1] Компания Naral собиралась создать сервис рассылки текстовых сообщений для отправки срочных извещений его подписчикам. Компания Verizon решила не допустить создания подобного сервиса из-за «противоречивых и сомнительных» данных,

[1] Адам Липтак (Adam Liptak) «Verizon reverses itself on abortion messages» (Verizon соглашается передавать сообщения на тему абортов), *New York Times* от 28 сентября 2007 года.

которые рассылаемые сообщения могли содержать. Возможность постоянного мониторинга хода предвыборной компании была сочтена правомерной, но для неполитических целей назначение сервиса считалось «противоречивым». Телефонные компании уже давно считаются общественной инфраструктурой. Как и железные дороги, телефонные компании защищены антимонопольным законодательством. Неважно, хотела компания Naral реализовать простой телефонный сервис или бесплатный номер, у Verizon не было особых оснований для отказа.

В мире битов нет разницы между текстовым сообщением и телефонным разговором. Все это – просто электрические колебания. Однако законодательство не успевает за развитием технологий. А законодательство об использовании телефонной связи отличается от законодательства, пытающегося регулировать работу Интернета.

На этот раз компании Verizon пришлось отступить, но ее политика осталась прежней. Телефонная компания может предпринимать любые меры, увеличивающие ее прибыль, в том числе решать, какие данные передавать по своим сетям. С технической точки зрения нет существенных различий между текстовыми сообщениями, телефонными звонками или любыми другими данными, передаваемыми по цифровым каналам связи.

Владение и конкуренция

Экономисты сказали бы, что без специального контроля биты склонны к *не-исключительности* (если они есть у нескольких человек, трудно уберечь их от остальных) и *не-конкуренции* (передавая их кому-то, я ничего не теряю). В своем письме о природе идей Томас Джефферсон подробно описал механизм данного явления. *Если природа создала что-то отличное от вещей, доступных каждому, то это есть проявление мыслительной сущности, называемой идеей. Индивидуум может исключительно владеть идеей до тех пор, пока хранит ее в тайне. Но в момент разглашения тайны идея переходит во всеобщую собственность независимо от воли владельца. Своеобразие данного явления в том, что никому не нужно конкурировать за идею, так как она не умаляется от разделения между мыслящими существами; каждому из них доступно все множество идей.*[1]

[1] Письмо Томаса Джефферсона Исааку Макферсону от 13 августа 1813 года, «Jefferson, Writings 13:333–35», *press-pubs.uchicago.edu/founders/documents/a1_8_8s12.html*.

Коан второй: совершенство – это естественное состояние

Человеку свойственно ошибаться. Когда в средневековых монастырях книги переписывались от руки, ошибки накапливались с каждой новой копией. Компьютеры и вычислительные сети работают иначе. Каждая копия совершенно повторяет оригинал. Если вы электронной почтой отправите другу фотографию, она будет схожа с оригиналом вплоть до мельчайших подробностей.

Компьютеры и вычислительные сети могут выходить из строя. Компьютер не может работать с отключенным питанием. Поэтому утверждение о том, что все копии совершенны, верно только относительно. Цифровые копии совершенны только при допущении, что они всегда доступны. Также теоретически возможно, что один или несколько битов сообщения исказятся при передаче. Однако сети не только передают биты, но и проверяют правильность доставки, и при обнаружении искажений пересылают биты повторно. Поэтому вероятность получения ошибочной копии сравнима с вероятностью того, что на ваш монитор упадет метеорит.

Возможность создания совершенных копий сильно повлияла на право, о чем будет подробнее сказано в главе 6. Когда звукозаписи распространялись на магнитофонных кассетах, никто не наказывал меломанов за перезапись. В этом не было нужды, потому что при многократном копировании каждая следующая копия была хуже предыдущей. Но сейчас, когда все копии одинаково совершенны и неотличимы от оригинала, тысячи людей подвергаются преследованиям со стороны гигантов медиаиндустрии. Биты довольно необычный вид собственности. Делясь с кем-то этой собственностью, вы делитесь со всем миром. Однако вы ничего не теряете, все ваши биты остаются при вас. Поэтому права владельца оригинальной информации – права на интеллектуальную собственность – почти невозможно юридически защитить.

Коан третий: изобилие порождает нищету

За последующие пять лет количество накопленной по всему миру информации может возрасти десятикратно. Парадоксальным образом, увеличение количества информации означает уменьшение ее доступности.

Один из моих знакомых недавно посетил клинику, услугами которой пользовался не один десяток лет. Прием вел молодой врач. Он показал пациенту множество графиков с данными химического анализа крови, переданными с домашнего медицинского прибора в компьютер клиники. Еще пять лет назад ни один медик не мог получить столько важных данных. Затем врач поинтересовался, проходил ли пациент тест на наличие стресса, и если проходил, то каков результат. Знакомый ответил, что результаты теста существуют и содержатся в медицинской *карте*. Врач не смог найти карту, и ему пришлось

довольствоваться весьма скудными показаниями самого пациента. Поскольку результаты теста не были оцифрованы и сохранены в *компьютере*, ситуация сложилась такая же, как если бы этих данных не существовало вовсе.

Так же бесполезна информация, содержащаяся на носителях, для которых нет устройств чтения. Быстрый прогресс в производстве устройств хранения привел к тому, что по вышеназванной причине данные, сохраненные на устаревших носителях, фактически перестали существовать. В главе 3 рассказано о том, как в XX веке было торжественно выпущено электронное издание Кадастровой книги Англии XI века и как данное издание смогло просуществовать только одну шестидесятую часть от срока существования оригинала.

Глава 4 посвящена поиску информации. Первоначально поисковые системы, вроде Google или Yahoo!, были не более чем любопытными вещицами и использовались ограниченным кругом людей для специфических целей. Развитие Всемирной паутины привело к созданию такого колоссального массива общедоступных данных, что поисковые системы оказались наиболее эффективным средством нахождения нужных сведений.

Сегодня многие скорее обратятся к поисковой системе, чем расспросят друзей или заглянут в книги. Для многих бизнесменов появление в верхних строках результатов поисковых систем – вопрос выживания. Ведь если сайт конкурента окажется на первой-второй странице результатов поиска, а ваш – на одной из последующих, то наиболее вероятно, что прибыль достанется конкуренту, так как большинство просто не заглянет дальше второй страницы. Мы можем думать, что жизнь идет своим чередом, если не увидим ничего особенного в содержании передовицы электронной газеты. Итог: если информация не может быть найдена[1] (причем быстро), то это аналогично тому, как если бы ее не существовало вовсе.

Коан четвертый: вычисления – сила

Производительность работы вычислительной техники обычно характеризуется количеством элементарных операций (например, операций сложения), которые могут быть выполнены в секунду. В начале 1940-х самые быстрые компьютеры могли выполнить 5 операций в секунду. Сегодня самые быстрые компьютеры способны выполнять триллионы операций в секунду. Опытным владельцам персональных компьютеров известно, что быстрый новый компьютер, купленный в текущем году, через год-другой будет считаться медленным и устаревшим.

---

[1] Это наблюдение появилось во второй половине 1990-х. См. Скотт Браднер (Scott Bradner) «How big is the world?» (Насколько велик наш мир?), *Network World* от 18 октября 1999 года. *http://www.networkworld.com/archive/1999b/1018bradner.html*.

В предыдущие тридцать лет производительность компьютерных микропроцессоров возрастала экспоненциально. Каждые несколько лет скорость работы компьютеров удваивалась. Это явление было следствием так называемого «закона Мура».

Закон Мура[1]

Гордон Мур, основатель корпорации Intel, обнаружил, что каждые несколько лет число транзисторов на кристаллах интегральных микросхем примерно удваивалось. Данное наблюдение получило название «закон Мура». Конечно, это не то же самое, что закон природы, вроде закона всемирного тяготения. Закон Мура является эмпирическим обобщением наблюдений за развитием технологий и своего рода вызовом дальнейшей изобретательности инженеров. В 1965 году Мур выдвинул предположение о том, что экспоненциальный рост производительности микросхем не может продолжаться бесконечно. Однако эта поразительная закономерность выполняется вот уже 40 лет. История не знает других примеров столь бурного роста.

Примерно с 2001 года производительность микропроцессоров растет уже не по закону Мура. Фактически производительность почти перестала возрастать. Но это не означает, что компьютеры не смогли поднять планку скорости. Новые технологии производства позволили размещать несколько процессоров в корпусе одной микросхемы. Это сделало возможным распараллеливание задач по процессорным ядрам и обеспечило повышение скорости работы компьютера. Данное новаторское решение оказалось почти таким же эффективным, как увеличение производительности одиночного микропроцессора. При этом технологии, обеспечившие подъем производительности, привели к удешевлению компьютеров.

Быстрый рост скорости обработки данных означает, что технические новинки быстрее проходят путь от создания прототипа в исследовательской лаборатории до отгрузки заказчику готовой серийной продук-

[1] Гордон Мур (Gordon Moore) «Ramming more components onto integrated circuits» (Увеличение числа элементов в интегральных схемах), *Electronics* № 8 от 19 апреля 1965 года, *ftp://download.intel.com/research/silicon/moorespaper.pdf*. Оригинал статьи заслуживает чтения – она составлена для популярного издания по электронике. Поздние публикации на тему «закона Мура» называют период удвоения полтора, а не два года. С весьма пространной (но не всегда убедительной) «разгромной» статьей можно ознакомиться по адресу *arstechnica.com/articles/paedia/cpu/moore.ars*.

ции. Роботы-пылесосы и самопаркующиеся транспортные средства, еще десять лет назад бывшие мечтой фантастов, уже сегодня доступны рядовому потребителю. В современных лабораториях промышленных корпораций и учебных заведений лучшие умы работают над разгадкой способностей, доступных пока только человеку. Возможность распознавания лица и речи приведет к созданию новых устройств, таких как телефоны, способные опознать звонящего, или камеры видеонаблюдения, не нуждающиеся в операторах. Истинная сила вычислительной техники заключается не в битах, а в возможности делать с ними все, что угодно.

Коан пятый: количество переходит в качество

Представьте себе экспоненциальное нарастание процесса, такое что его характеристики удваиваются за определенный период. Если ваши банковские сбережения будут удваиваться каждый год, то за десять лет они увеличатся больше чем в тысячу раз, а за двадцать лет – больше чем в миллион раз. При более приближенной к реальности ставке в 5% на это потребуется в 14 раз больше времени. Нечто похожее происходит во время эпидемий, когда один зараженный человек заражает несколько здоровых.

Когда что-то растет по экспоненте, поначалу может долго казаться, что ничего не происходит. А без постоянного наблюдения покажется, что пока не смотрел, все радикально изменилось.

По этой причине эпидемии начинаются незаметно, вне зависимости от того, насколько катастрофично они разрастаются потом. Представьте себе, что один больной заражает двух здоровых. На следующий день каждый из этих двоих тоже заразит по два человека. Через неделю таким путем будут заражены 128 человек. Однако для нации численностью 10 миллионов это будет незаметно. Через две недели заболеют три человека из каждой тысячи, что опять-таки почти незаметно. Но еще через неделю непрерывного заражения будут больны 40% населения, и общество окажется на грани уничтожения.

Экспоненциальный рост происходит плавно и неотвратимо. От едва заметных изменений до безнадежных проходит совсем немного времени. Экспоненциальное развитие может внезапно и полностью изменить мир. На определенной стадии количественные изменения переходят в качественные.

Попробуем выяснить, сколько времени нужно, чтобы остановить распространение болезни. Нашей гипотетической эпидемии потребовалось три недели, чтобы победить нацию. В какой момент распространение эпидемии было вполовину менее разрушительным? Ответ: *не* «через полторы недели». Ответ: *на следующий день*. Предположим, на разработку и производство вакцины хватит недели. Еще несколько дней уйдут на вакцинацию населения. Если принять указанные меры

сразу же, при обнаружении носителя инфекции (то есть в первый день воображаемого эксперимента), то эпидемия будет остановлена на второй неделе, когда число зараженных достигло примерно двух тысяч. Но кто разглядит симптомы *эпидемии* у нескольких тысяч человек в десятимиллионной нации? Когда эти симптомы все же будут выявлены, может быть уже поздно, и любые меры окажутся бесполезными.

История цифровой экспансии пестрит примерами нераспознанных признаков перемен и взрывного наступления последствий. Те, кто распознает признаки готовящегося наступления битов чуть раньше остальных, может получить огромное преимущество. Те, кто хоть немного замешкается, будут разбиты, не успев дать отпор. Примером этого может служить история развития цифровой фотографии.

В 1983 году на Рождество можно было купить цифровой фотоаппарат, подключаемый к домашнему компьютеру IBM PC или Apple II.[1] В новинке не было никакой секретности, и приобрести такое устройство мог каждый. Однако новинка не прижилась. Первые цифровые фотоаппараты были слишком громоздки, чтобы можно было носить их в кармане, и памяти в них было явно недостаточно для большого количества снимков. Даже 14 лет спустя пленочные фотоаппараты прочно занимали рынок.[2] В начале 1997 года стоимость акций компании Kodak выросла на рекордные 22% за квартал «вследствие успешных продаж пленки и фотобумаги... <и> роста киноиндустрии», как говорилось в отчете для прессы. Впервые за 8 лет прибыль по дивидендам компании поднялась. Однако к 2007 году емкость карт памяти значительно увеличилась, процессоры стали более быстрыми и компактными, а сами цифровые фотоаппараты подешевели. В итоге, фотокамеры стали маленькими компьютерами. А компания Kodak, чье имя было синонимом искусства фотографии, превратилась в тень самой себя. Число сотрудников бывшего гиганта фотоиндустрии сократилось до 30 тысяч человек, что составляло одну пятую часть от штата «золотых» 1980-х. Действие закона Мура обошлось компании Kodak больше чем в 3 миллиарда долларов.[3]

В быстро меняющемся мире битов приходится обращать внимание на мельчайшие изменения и принимать соответствующие меры.

---

[1] Кэрол Ранали (Carol Ranalli) «Digital camera lets computers see» (Цифровая фотокамера позволяет компьютерам видеть), *Infoworld* от 21 ноября 1983 года.

[2] «Kodak, GE, Digital report strong quarterly results» (Kodak, GE, Digital отчитываются о высоких квартальных прибылях), *Atlanta Constitution*, 17 января 1997 года.

[3] Клаудия Дейч (Claudia H. Deutsch) «Shrinking pains at Kodak» (Kodak сокращает расходы), *New York Times*, 9 февраля 2007 года.

Коан шестой: ничто не исчезает бесследно

2 000 000 000 000 000 000 000 (два секстиллиона).

Таково, по оценкам специалистов, примерное количество битов, созданных и хранимых по состоянию на 2007 год.[1] Емкость носителей, следуя соответствующей версии закона Мура, удваивается каждые 2–3 года. В настоящее время можно хранить все создаваемые биты, хотя есть мнения, что к 2011 году количество информации превысит емкость доступных носителей.

В финансовом мире федеральное законодательство *требует* хранить огромные массивы данных для аудита и расследований финансовых афер. Экономическая конкуренция побуждает компании накапливать все поступающие данные, чтобы удержаться в бизнесе. Базы данных розничной сети Wal-Mart обрабатывают десятки миллионов транзакций ежедневно. Для каждой транзакции сохраняются дата, время, название товара, адрес склада, цена, данные о покупателе и способ оплаты. Эти данные незаменимы для максимально эффективного обслуживания покупателей. Так создаются приманки в виде дисконтных карт и подарочных сертификатов – покупатели думают, что владельцы супермаркета ценят лояльность клиентов, но на самом деле владельцы ценят знания о предпочтениях покупателей, поскольку такие знания позволяют закупать популярные товары и увеличивать доходы. Такова цена права на частную жизнь: хотите сохранить в тайне свои предпочтения, – платите больше.

Возможность хранения сверхбольших баз данных изменяет наше представление о том, что вообще могут знать о нас посторонние. Возьмем такую простую вещь, как остановка в отеле. Когда вы регистрируетесь, вам выдают пластиковую карту – ключ к электронному замку вашего номера. Потеряв карту, вы просто сообщаете об этом администрации и получаете новую. Поскольку такую карту всегда можно блокировать, риск того, что кто-то другой сможет пробраться в ваш номер с помощью потерянной карты, значительно ниже, чем при использовании обычного дверного замка. С другой стороны, владелец отеля располагает посекундными сведениями о вашем местонахождении в пределах отеля, находитесь ли вы в своем номере, спортзале или бизнес-центре или вышли через черный ход. Та же база данных может в любой момент сообщить, какую еду и напитки вы заказывали в номер, кому и когда звонили по внутренней связи и что купили в магазине подарков. Эти данные могут быть объединены с миллионами других, проанализированы и переданы владельцам сети отелей или фитнес-центров. Эти

---

[1] Доклады IDC, спонсируемые EMC: «The Expanding Digital Universe», март 2007 года, *www.emc.com/about/destination/digital_universe/pdf/Expanding_Digital_Universe_IDC_WhitePaper_022507.pdf;* «The Diverse and Expanding Digital Universe», март 2008 года, *www.emc.com/collateral/analyst-reports/diverse-exploding-digital-universe.pdf.*

данные также могут быть утеряны, украдены или запрошены правоохранительными органами.

Преимущества, предоставляемые подобными базами данных, побуждают к еще большему накоплению информации. Раньше свидетельство о рождении содержало только имя, дату и место рождения ребенка и родителей плюс род занятий родителей. Теперь электронная запись о рождении может включать такие сведения, как: обнаружен ли у матери генитальный герпес и другие болезни; сколько мать курила/выпивала во время беременности; номера социального страхования родителей. Здесь кроются богатейшие возможности для медицинских исследований, равно как и возможности для злого умысла или катастрофической неразберихи в случае неумышленной потери данных.

Все данные могут храниться вечно, если от них методически не избавляться

И все данные могут храниться вечно, если от них методически не избавляться. Пока что носителей для всех накопленных данных хватает. Поскольку данные дублируются для надежности или их копии передаются для каких-то нужд, было бы глупо предполагать, что некие данные вдруг навсегда исчезнут. Интернет состоит из миллионов связанных компьютеров. Если вы пустите данные в Сеть, то не сможете их удержать. Жертвы взломщиков паролей и сертификатов вынуждены ежедневно удалять из своих баз ложные записи. Кажется, что этому нет конца.

Коан седьмой: биты движутся быстрее мысли

Интернет появился раньше персональных компьютеров и высокоскоростных оптоволоконных кабелей, которые образуют его теперь. В 1970 году небольшая вычислительная сеть ARPANET соединила несколько компьютеров крупнейших университетов и Департамента обороны США. Никому из ее создателей и не снилась вычислительная сеть, соединяющая миллионы компьютеров и содержащая самую разнообразную информацию, доступную в мгновение ока в любом конце света. В дополнение к росту скорости обработки информации и объема ее носителей Всемирная сеть сама испытала экспоненциальный рост количества входящих в нее компьютеров и скорости обмена данными.[1]

Бурный рост Интернета радикально изменил многие виды бизнеса. Звонки службы поддержки теперь часто перенаправляются в Индию не только потому, что в этой стране *всегда* самая дешевая рабочая сила, но и потому, что Интернет позволил удешевить международные звонки. Телефонные переговоры о бронировании авиабилетов или возврате партии текстильной продукции направляются в Индию, по-

[1] Данные консорциума Internet Systems Consortium «ISC Domain Survey: Number of Internet Hosts», *www.isc.org/index.pl?/ops/ds/host-count-history.php*.

скольку пересылка битов, кодирующих вашу речь, происходит почти мгновенно и стоит всего ничего. Те же средства используют и профессиональные службы. Ваши рентгеновские снимки, сделанные в больнице в Айове, будет изучать специалист в другой части света. Цифровой снимок обойдет полмира и вернется обратно быстрее, чем рентгеновские лучи пройдут расстояние между этажами больничного корпуса. Когда вы удаленно заказываете еду в фаст-фуде, сотрудник, принимающий заказ, может находиться в другом штате. Из другого штата ваш заказ отправляется на кухню, до которой идти всего несколько метров, но вам не суждено знать, какой путь он проделает. Такое распределенное управление произвело революцию в экономике: бизнесмены поняли, что выгоднее не перемещать работников, а пересылать биты.

В мире битов, в котором постоянно пересылаются сообщения, иногда возникает ощущение, что расстояний нет. Результаты исчезновения расстояний могут быть поразительными. Один из нас, будучи деканом американского колледжа, видел убитого горем отца, принимавшего соболезнования в связи со смертью дочери. Это было печально, но отнюдь не необычно, если бы не удивительная деталь. И отец, и дочь жили в Массачусетсе, но соболезнования, перед тем как попасть к отцу, обошли чуть ли не полмира. Новости, даже о глубоко личных событиях, едва попав в Интернет, расходятся в мгновение ока. Осенью 2007 года, когда правительство Мьянмы подавило восстание буддийских монахов, телевизионные станции по всему миру транслировали это событие, которое очевидец снял мобильным телефоном. Возможно, именно эти кадры стали причиной смены официальной позиции Белого дома. Восстание в Мьянме показало, насколько мощен информационный контроль, если информация – это просто биты. Эта история исчезла с первых страниц газет лишь тогда, когда правительство смогло полностью контролировать Интернет и базовые станции сотовой связи.[1]

Возможности создания огромного числа связей породили ошибочное впечатление о явлении, называемом «Киберпространство», – стране, где нет границ, где люди всего мира могут свободно общаться друг с другом. К сожалению, в реальности не все так просто. Национальные законодательства очень сильно различаются. Если книга куплена в Великобритании, то по британскому законодательству автор и издатель книги несут ответственность за возможную клевету независимо от их гражданства и места проживания. В Великобритании подсудимый должен доказывать свою невиновность; в США сторона обвинения должна доказывать вину подсудимого. Темная сторона всемирной

[1] Сет Майдэнс (Seth Mydans) «Monks are silenced, and for now, Internet is, too» (Монахи успокоились, и Интернет тоже), *New York Times*, 4 октября 2007 года. года; OpenNet initative, «Pulling the Plug: A Technical Review of the Internet Shutdown in Burma» (Выдернуть штекер: технический обзор отключения Интернета в Бирме).

цифровой экспансии заключается в том, что информация становится менее доступной, даже если ее защита обеспечивается законом (мы еще вернемся к этой теме в главе 7). Издатели опасаются «миграции клеветы», так как законодательство в странах с ограниченной свободой слова направлено на преследование авторов из более либеральных стран. Возможно, проще опубликовать единственную редакцию произведения для возможности продажи где угодно[1], обрезав книгу так, чтобы ее содержание не могло никого задеть.

Добро и зло, перспективы и риски

Армия битов захватывает все больше жизненного пространства, поэтому мы должны знать, кто кует для нее оружие. Методы, которыми нам преподносятся технологии, наши способы применения этих технологий и последствия повсеместного распространения цифровой информации зависят теперь не только от технических специалистов. Правительства, корпорации, университеты и другие общественные институты должны сказать свое слово. Простые граждане, которым небезразлична судьба общества, не должны оставаться в стороне. Каждый год в правительственных кабинетах и законодательных собраниях, полицейских участках, банках, страховых компаниях, отделах закупок розничных сетей и аптек принимаются важные решения. Мы должны поднимать культуру ведения дискуссии, следя за тем, чтобы технические решения соответствовали потребностям нации.

Читателю предлагается принять два постулата. Первый состоит в том, что сами по себе технологии ни хороши, ни плохи, но в чьих-то руках они могут либо дать нам свободу, либо поработить. Второй постулат гласит, что новые технологии изменяют общество, и эти изменения несут в себе как риски, так и перспективы. Все граждане, а также социальные структуры должны высказать свое мнение о пользе или вреде от очередных нововведений.

Сами по себе технологии ни хороши, ни плохи

Любую технологию можно использовать как во благо, так и во зло. Ядерные реакции могут давать электрическую энергию, а могут быть применены в оружии массового уничтожения. Технология шифрования может исключить возможность чтения вашей электронной почты любителем покопаться в грязном белье. Но та же технология шифрования может надежно скрыть планы террористов. Файлообменные сервисы могут предоставить электронные учебники тем студентам, которые не могут позволить себе купить бумажные. Но те же сервисы могут привести к массовому нарушению авторских прав. Программы,

[1] Рэйчел Донадио (Rachel Donadio) «Libel without borders» (Клевета без границ), *New York Times* от 7 октября 2007 года.

предназначенные для коррекции дефектов цифровых фотографий, помогают скрываться распространителям детской порнографии.

Ключом к управлению морально-этическими последствиями развития технологий при сохранении существующих тенденций является разумный контроль, без необоснованных *запретов или ограничений*.

Разве не чудо, что любой владелец смартфона может практически из любой точки земного шара использовать мощь поисковых систем для получения ответов на свои вопросы? Общество все быстрее сбрасывает путы географических и социальных ограничений на право доступа к информации.

Но те же силы, что создали это чудо, могут быть использованы для отслеживания отдельных людей и контроля их действий и получаемой ими информации. Можно управлять работой поисковой системы и выдавать только желательные для ее владельца результаты. Многие пользователи Интернета не в курсе, что серверы посещаемых ими сайтов способны архивировать все запросы. Технически возможно создать точный журнал посещений веб-сайтов, неважно, искали ли вы книгу в электронной библиотеке или интернет-магазине, заходили ли на сайт аптеки поинтересоваться ценой на лекарство или за советом по его применению. Собранные сведения можно использовать как для маркетинговых исследований, так и для создания «черных списков» или для шантажа.

Неразвитость соответствующего законодательства способствует сбору нужных данных и их тайной цензуре. Недавно принятые федеральные законы, такие как «Патриотический акт» (USA PARTIOT Act)[1], предоставили спецслужбам США исключительные права на просмотр любых, даже вроде бы не относящихся к делу данных для поиска «подозрительной активности» потенциальных террористов или следов менее опасных преступлений. вроде упоминавшегося в начале главы дела губернатора Нью-Йорка.

Хотя во Всемирной паутине насчитываются миллионы узлов, закона и порядка в ней не больше, чем в каком-нибудь богом забытом городишке на окраине Дикого Запада.

---

[1] «USA PATRIOT Act» – Патриотический акт, или Акт патриота США 2001 года (полное название «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act» – «Акт об объединении и усилении Америки посредством применения адекватных средств, необходимых для предотвращения и пресечения террористических актов»), подписанный президентом Джорджем Бушем в октябре 2001 года. Регистрационное обозначение: Public Law 107–56. Закон расширил полномочия правоохранительных органов по наблюдению за электронными коммуникациями и записями в целях борьбы с внутренним терроризмом.

Черные и белые списки

В мире битов провайдеры могут создавать так называемые черные и белые списки. Для лиц, занесенных в черные списки, доступ к сервисам отключается, оставаясь открытым для всех остальных. К примеру, владелец интернет-аукциона может включать в свой черный список покупателей, не оплативших покупки. Другие поставщики услуг, располагающие более подробной информацией о посетителях, могут создавать черные списки по множеству критериев. Для лиц, занесенных в белые списки, доступ к сервисам открыт, будучи при этом закрытым для всех остальных. Например, служба онлайн-новостей может быть открыта только для подписчиков печатного новостного издания, в то время как всем остальным самые свежие новости недоступны.

Новые технологии несут в себе как риски, так и перспективы

С помощью больших дисковых накопителей, позволяющих любому владельцу домашнего компьтера изучать статистику тысяч бейсбольных матчей, тот, кто получил доступ к секретным данным некой организации, может угрожать ее безопасности. Свободный доступ посредством Интернета к картам аэрофотосъемки окажет неоценимую помощь преступникам, планирующим ограбление особняка. Если полиция получит журналы запросов на эти карты, то сможет быстрее предотвратить или раскрыть преступление.

Непрерывно нарастающая экспансия информационного потока изменяет даже наиболее далекие от цифровых технологий сообщества. Уже редко можно встретить «бильярдных шулеров». Раньше путешествующие мастера кия, играя на деньги под видом заезжих провинциалов, могли обчистить местных чемпионов.[1] Теперь имя и фотография каждого нового успешного игрока заносятся в галерею сайта *AZBilliards.com* и каждый может узнать, сколько побед на счету у соперника.

Социальные сети, такие как *Facebook*, *MySpace* и *match.com*, приносят их создателям огромные прибыли. Также социальные сети способствовали возникновению множества дружеских связей, заключению браков и деловых союзов. Однако не все те, кто представляется вашим другом, являются ими на самом деле. Социальные сети облегчают возможность людям с нечистой совестью манипулировать более доверчивыми, одинокими, пожилыми или юными людьми.

---

[1] Йон Вертхейм (Jon Wertheim) «Jump the Shark» (Обставить знатока), *New York Times* от 24 ноября 2007 года.

В 2006 году Мэган Майер, тринадцатилетняя девочка из городка Дардин Прэйри (штат Миссури), познакомилась в Сети с шестнадцатилетним парнем с ником «Джош». Когда «Джош» внезапно написал Мэган: «Ты плохая и все тебя ненавидят. Мир станет лучше без тебя», – девочка в отчаянии совершила самоубийство. Произошло ужасное событие, притом что никакого «Джоша» реально не существовало. «Джош» был одной из учетных записей в социальной сети MySpace. Кто же создал эту запись? В первоначальном отчете полиции сообщалось, что мать девочки-соседки призналась в участии в создании данной учетной записи. Позднее ее адвокат переложил ответственность на того, кто работал на подзащитную.[1] Но вне зависимости от того, кто отправил роковое сообщение, следствие потратило немало усилий, пытаясь определить, было ли вообще нарушено какое-либо положение закона. «С помощью MySpace я могу завести знакомство с кем угодно, а потом распространять о каждом грязные слухи. И мне за это ничего не будет» – подвела итог мать Мэган.

Наряду с широкими возможностями быстрого обогащения, Интернет позволил по-новому проявиться темной стороне человеческой натуры. Некоторые из этих проявлений, как например, случай с Мэган Майер, могут даже не подпадать под определение преступления. Проблема усугубляется тем, что Америка традиционно считается страной с почти не ограниченной свободой слова.

Возможность связаться через Интернет с кем угодно позволяет не доставлять людей на работу, а доставлять работу людям. Результат – огромные перспективы для бизнеса у тех, кто может ими воспользоваться, и новые предприятия по всему миру. Есть и другая сторона медали – работа уходит к другим подрядчикам.

Каждый из нас может по-новому взглянуть на свою работу или на какую-то другую сторону жизни и вовремя задать себе вопрос: угрожает ли цифровая экспансия в данном случае новыми потерями или предоставляет новые возможности?

Наше путешествие по карте экспансии цифровых технологий началось с той грани общества, которую нашествие битов почти полностью обра-

[1] Стив Покин (Steve Pokin) «A real person, a real death» (Реальная личность, реальная смерть), *St. Charles Journal* от 10 ноября 2007 года; Кристофер Мааг (Christopher Maag) «A hoax turned fatal draws anger but no charges» (Автор розыгрыша, вызвавшего фатальный приступ отчаяния, не понесет наказания), *New York Times* от 28 ноября 2007 года; Ребекка Кэткарт (Rebecca Cathcart) «MySpace is said to draw subpoena in hoax case» (MySpace приказано явиться в суд по делу о розыгрыше), *New York Times* от 10 января 2008 года.

тило в руины, – с неприкосновенности частной жизни. Наслаждаясь преимуществами доступа к почти неограниченному количеству информации, мы чувствуем утрату той защиты, которую предоставляла свобода от постоянного наблюдения. И мы не знаем, чем восполнить потерю. Добро и зло, перспективы и риски, получаемые одновременно с новыми технологиями, идут бок о бок, когда сведения о каждом становятся доступны всем. В мире постприватности мы стоим под всевидящим электронным оком – и иногда чувствуем странное удовлетворение от происходящего.

Глава 2 | Под всевидящим электронным оком

Оставь надежду на неприкосновенность частной жизни, всяк сюда входящий

1984 – реальность, но мы рады

7 июля 2005 года Лондон был потрясен серией из четырех взрывов, из которых три прогремели в метро и один – в двухэтажном автобусе.[1] Транспортная система города была атакована в точно рассчитанное время, когда на улицах и в метро было наиболее людно. В результате взрывов погибли 52 человека и больше 700 получили ранения.

Службы безопасности Лондона были начеку. Город готовился к саммиту стран «Большой восьмерки», а в суде слушалось дело ортодоксального мусульманского священника Абу Хамза эль-Масри. Сотни тысяч камер видеонаблюдения не могли предотвратить теракт, но им удалось зафиксировать его исполнителей.[2] Снимки были мгновенно разосланы по всему миру. Обработав около 80 тысяч кассет с записями, полиция смогла восстановить действия смертников за две недели до теракта.

Роман «1984» Джорджа Оруэлла был опубликован в 1948 году. Спустя годы название книги стало синонимом общества постоянного наблюдения, общества, в котором люди лишены свободы и частной жизни:

> ...все в городе выглядело бесцветным – кроме расклеенных повсюду плакатов. С каждого заметного угла смотрело лицо черноусого. С дома напротив тоже. СТАРШИЙ БРАТ СМОТРИТ НА ТЕБЯ.[3]

Реальный 1984 год наступил около четверти века назад. Сегодня «телекраны» Старшего брата кажутся детскими игрушками. Оруэлл описал Лондон, нашпигованный телекамерами. Сегодня их в Лондоне около

---

[1] Одно из самых подробных описаний этих событий можно найти в Википедии, *en.wikipedia.org/wiki/7_July_2005_London_bombings*.

[2] Сара Лайал (Sarah Lyall) «London Bombers Visited Earlier, Apparently on Practice Run» (Лондонские смертники предварительно отработали свои действия), *New York Times* от 21 сентября 2005 года.

[3] Цит. по: Джордж Оруэлл «1984» и эссе разных лет. М.: Прогресс, 1989.

полумиллиона. В Великобритании примерно одна камера на дюжину человек. Электронные глаза, расположенные на стенах зданий или на специальных опорах, ежедневно фиксируют каждого лондонца в среднем сотни раз.

Однако цифровой мир гораздо обширнее, чем смог вообразить писатель-фантаст. Оруэлл не предполагал, что камеры слежения отнюдь не составляют львиную долю сегодняшних технологий «Старшего Брата». Существуют десятки других источников информации, и все они вносят свой вклад в общую картину тотального контроля.

Сотовые операторы могут сказать не только кому и когда вы звонили, но и где находится ваш телефон. Кредитная карта сообщит не только где вы потратили ваши деньги, но и на что вы их потратили. Банк хранит журнал ваших транзакций не только ради корректности баланса, но и для того, чтобы спецслужбы могли узнать, не делали ли вы подозрительно крупные взносы. Цифровая экспансия повсюду насадила битов-шпионов: они узнают, какую одежду вы носите, каким мылом моетесь, по каким улицам ходите, а если вы предпочитаете автомобиль, – они и это узнают.

Хотя у оруэлловского Старшего Брата были видеокамеры, но у него не было поисковых систем, которые собирали бы разрозненные биты в цельную картину, отделяя зерна от плевел. Куда бы вы ни пошли, вы оставляете цифровые следы, из которых компьютеры невообразимой вычислительной мощности восстанавливают весь ваш путь. Электронные машины формируют целостный портрет вашей личности: известно, кто вы, чем занимаетесь и с кем делитесь своими догадками.

Возможно, достижения современных технологий не особенно удивили бы Оруэлла. Он не мог знать о миниатюризации электроники, но, вероятно, догадался бы, что ассортимент средств слежения за личностью будет только возрастать.

Нынешний мир отличается от мира, описанного Оруэллом, еще одним свойством. Обитатели цифрового мира сами стремятся существовать в нем. Потеря анонимности считается небольшой платой за эффективность, удобство и ценовые скидки. Согласно отчету Pew Internet Project за 2007 год[1] «60% пользователей Интернета не интересуются тем, сколько информации о них доступно в Сети». Многие публикуют мельчайшие подробности своей жизни, делая эти сведения доступными всему миру[2], даже если никто об этом не просит. 55% подростков и 20% взрослых обзавелись учетными записями в социальных сетях.

---

[1] «Digital Footprints» (Цифровые следы), «Online identity management and search in the age of transparency» (Управление сетевой идентификацией и поиск в век открытости), Pew Internet & American Life Project, 2007.

[2] Там же.

Из них треть подростков[1] и половина взрослых никак не ограничивают просмотр персональных данных.

Общественные организации за неприкосновенность частной жизни

Ряд организаций, как новых, так и не очень, озабочены проблемой потери неприкосновенности частной жизни. Наиболее влиятельные из них в США: Американский союз гражданских свобод (American Civil Liberties Union, ACLU, *www.aclu.org*); Информационный центр электронной конфиденциальности (Electronic Privacy Information Center, EPIC, *epic.org*); Центр демократии и технологий (Center for Democracy and Technology, CDT, *www.cdt.org*); Фонд электронной безопасности (Electronic Frontier Foundation, EFF, *www.eff.org*).

В воображаемом Лондоне Джорджа Оруэлла только О'Брайен и другие члены внутренней партии обладали правом отключать телекраны. Постоянное сознание того, что за ними наблюдают, вселяло беспокойство и тревогу в души членов выдуманного общества. В современном реальном обществе граждане сами добиваются внимания. Люди не только не задумываются об этой проблеме, но зачастую даже не знают о ней; а если знают, то смиряются, считая, что избежать наблюдения «Старшего Брата» могут только полные отшельники. Часто люди считают, что преимущества положения перевешивают недостатки. В вымышленном Лондоне, похожем на Москву сталинской эпохи, граждане шпионили друг за другом. Сегодня можно самому стать «Младшим Братом» и шпионить, не выходя из дома. Пользователи Интернета используют поисковые системы, чтобы получать информацию о своих детях, супругах, соседях, коллегах, врагах и друзьях. Этим занимается больше половины взрослых пользователей.

Стремительная экспансия цифровых технологий радикально уменьшила количество наших потенциальных секретов и сместила границы представлений о том, что следует хранить в тайне. Забавно, что наши представления о неприкосновенности частной жизни стали более расплывчатыми одновременно со все более широким распространением технологий шифрования и скрытия информации. Безусловно, мы всё еще не закрываем глаза на вторжения, которые десять лет назад могли вызвать шок. Однако технологии слежения отбросили покров секретности и предпочли тактику малых побед. Постоянно

[1] Отчет Pew Internet & American Life Project «Teens and Social Media» (Подростки и социальная медиасреда) от 19 декабря 2007 года, стр. 13, *www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf*.

наращивая свое влияние сразу на нескольких фронтах, армии цифровых устройств господствуют повсюду. Многие устройства стали дешевле, удобнее и меньше. Люди не задумываются о том, что полезные потребительские товары – это средства слежения. К примеру, если бы мобильные телефоны с фотокамерами были только у полиции, мы бы забеспокоились. Но поскольку они доступны каждому (ура! можно порадовать друзей фотографиями со вчерашней вечеринки!), немногие задумываются о том, кто, когда и зачем может так же легко фотографировать их самих.

Развитие общества, поддержанное технологиями, ориентированными на рядового потребителя, в свою очередь, способствовало более спокойному восприятию новых технологий. Так развитие общества и технологий идут рука об руку. Между прочим, международный терроризм привлекает к себе больше внимания в демократических обществах, более лояльных к применению крайних мер ради усиления безопасности. На фоне корпораций, пытающихся выжать из нас больше денег, и правительств, пытающихся защитить нас, сложно различить голоса борцов за свободу личности и гражданские права, предупреждающих о том, что все больше информации о нас попадает в чужие руки.

Давайте поэтапно проследим всю историю уничтожения неприкосновенности частной жизни. Во-первых, надо описать вспомогательные технологии, устройства и вычислительные процессы, ради которых мы так легко расстались со своим правом на частную жизнь. Многие из этих технологических достижений хорошо знакомы, другие менее известны.

Во-вторых, проведем анализ того, как мы обменяли на иллюзорные удобства (или просто отбросили) наши естественные права. Это происходило как без нашего участия, так и с нашей собственноручной помощью. Как результат, сегодняшнее понятие частной жизни сильно отличается от того, каким оно было тридцать лет назад. В-третьих, мы обсудим, как под действием цифровой экспансии изменилось направление развития общества, что, в свою очередь, вызвало дальнейшее развитие цифровых технологий.

В заключение мы обратимся к главным вопросам: что значит понятие неприкосновенности частной жизни в мире, нашпигованном битами-разведчиками? Есть ли хоть малая надежда сохранить что-либо в тайне в условиях, когда биты повсюду перемещаются, хранятся, копируются и распространяются? И если мы не можем – или не хотим – хранить в тайне наши персональные данные, то как сможем уберечь себя от опасностей окружающего мира, в котором реальная и цифровая составляющие неразрывно сплелись? Бессильные скрыться от надзора тысяч электронных глаз, можем ли мы уберечься от зла, от которого раньше нас хранила неприкосновенность частной жизни?

Следы ног и отпечатки пальцев

Живя обычной жизнью и делая свою работу, мы оставляем следы ног и отпечатки пальцев. Следы можно увидеть на полу, на снегу или на песке. И сравнив форму отпечатков с рисунком подошвы, любой сможет проследить наш путь. Отпечатки пальцев еще более информативны, так как уникальны. Ничего не случится, если оставить свои отпечатки на мебели или посуде. Но тот, кто готовит преступление, понимая всю важность дактилоскопии, не забудет о перчатках.

В цифровой мире за каждым из нас тянется длинный шлейф «следов» и «отпечатков». Мы оставляем следы намеренно или неосознанно. Идентификационные данные могут быть прочитаны и использованы полицией или спецслужбами. Но большинство пользователей не считает себя преступниками, поэтому не заботится о сохранении конфиденциальности. Часто пользователи не задумываются о том, что оставляют незаметные следы, доступные злоумышленникам, которые специально ищут подобную информацию, чтобы заработать на ней, как правило, незаконно. Поэтому ради собственной безопасности важно понимать, где и как вы оставляете цифровые следы.

Улыбайтесь, мы вас снимаем!

У Старшего Брата были тысячи камер, возможно не меньше, чем их в Лондоне сегодня. Но все это не сравнится с количеством фотокамер в мобильных телефонах подростков по всему миру. Этот факт хорошо иллюстрирует история расследования дела Джеффри Бермана.

В начале декабря 2007 года мужчина примерно шестидесяти лет совершил несколько нападений на девушек в общественном транспорте Бостона. Одной из жертв удалось сфотографировать преступника на свой мобильный телефон и сбежать. Один щелчок – и через несколько часов снимок появился в Интернете и на городском телевидении. В течение дня Берман был арестован по обвинению в совершении серии преступлений. «Конечно, наши сотрудники в штатском регулярно патрулируют общественный транспорт, но проверить всё невозможно, – заявил начальник транспортной полиции Бостона. – Снимок, который смогла сделать девушка, оказался поистине бесценным».[1]

Может показаться, что у этой истории счастливый конец – по крайней мере для последней жертвы. Однако всеобщее распространение доступных фотокамер вкупе со свободным доступом в Интернет возрождает традицию линчевания и создает новых «Младших Братьев», каждый из которых может быстро и недорого стать следователем, судьей и исполнителем приговора в одном лице. Что, если Берман был невино-

[1] О'Райен Джонсон (O'Ryan Johnson) «Green Line Groper Arrested» (Убийца девушек арестован), *Boston Herald* от 8 декабря 2007 года.

вен[1], а поспешно сделанный цифровой снимок запечатлел не то лицо? Пользователи, ведущие блоги, могут опозорить рядовых граждан на весь мир.

Нежелательный взгляд

В книге Джеффри Розена (Jeffrey Rosen) «The Unwanted Gaze» (Нежелательный взгляд), Vintage, 2001 детально описаны многие способы, с помощью которых правоохранительные органы вторгаются в нашу личную жизнь.

В июне 2005 года в Корее девушка позволила своей собаке облегчиться в вагоне метро и отказалась убирать за ней, хотя окружающие даже предлагали свою помощь.[2] Этот эпизод был снят на камеру мобильного телефона другой пассажиркой, и фотографии выложены на популярном сайте. Вскоре личные данные этой девушки стали известны всем, и ее стали называть не иначе, как «дама с вонючкой» (по-корейски «гэй тонг нье»). Владелице собаки пришлось даже покинуть университет. Случай попал в Википедию (*http://en.wikipedia.org/wiki/Dog_poop_girl*).

До цифрового нашествия об этой истории могли знать только другие пассажиры злополучного вагона. В том, что какая-либо история может таким же образом обойти весь мир и создать ее участникам подобную печальную известность, мало хорошего.[3]

Есть множество бесплатных сайтов, позволяющих видеть, что происходит в различных местах по всему миру. Вот некоторые из них:

www.camvista.com
www.earthcam.com
www.webcamworld.com
www.webworldcam.com

---

1 «Newton man arraigned in groping case» (Обвиняемый в убийстве девушек предстал перед судом), *Boston Globe* от 11 декабря 2007 года.

2 Сара Боксер (Sarah Boxer) «Internet's Best Friend (Let Me Count the Ways)» (Лучший друг Интернета (позвольте мне перечислить все способы)), *New York Times* от 30 июля 2005 года.

3 Джонатан Крим (Jonathan Krim) «Subway Fracas Escalates Into Test of the Internet's Power to Shame» (Скандал в метро доказал способность Интернета опозорить кого-либо), *Washington Post* от 7 июля 2005 года.

В случаях, подобных описанному, кто-то совершает ошибку, которую могут запечатлеть окружающие. Но в Интернете можно найти множество снимков со всего мира, изображающих сцены обычной жизни. Сервис Google Street View позволяет вам, сидя в чайной где-нибудь в Таджикистане, увидеть машину, припаркованную у моего подъезда, случайно сфотографированную камерой Google (возможно, несколько месяцев назад). Из Сеула вы можете с интервалом обновления в несколько секунд смотреть, что в это время делается на Пикадилли или в стриптиз-клубе в Лас-Вегасе. Эти сцены всегда были доступны публике, но цифровые камеры и Всемирная паутина придали новое значение слову «публикация».

Также цифровая камера – это больше, чем просто камера. Как известно, книга «Гарри Поттер и Дары Смерти» стала последней в серии о приключениях Гарри Поттера. Выход книги был одним из самых ожидаемых событий, очереди из поклонников выстраивались у дверей книжных магазинов по всему миру. Однин из поклонников, раздобыв предварительный экземпляр, старательно сфотографировал все страницы и выложил в Интернет с открытым доступом всю книгу еще до официально запланированного выхода. Это, несомненно, был подвиг ради любви, но, так же несомненно, это было вызывающее нарушение авторских прав. Поклонник не сомневался, что всего лишь отправил на сервер массив битов, составляющих изображения, но это было не совсем так.

Все фотографии содержали цифровые «отпечатки», так как любая цифровая камера сохраняет вместе с данными собственно изображения еще и служебную информацию. Эта служебная информация (метаданные), известная как «Формат файлов для переносимых изображений» (Exchangeable Image File Format, EXIF), содержит настройки камеры (скорость затвора, апертура, сжатие, сам снимок, цветовая модель, ориентация), дату и время съемки, а также модель и заводской номер камеры, в данном случае – Canon Rebel 350D, номер 560151117. Если бы поклонник зарегистрировал свою камеру, купив ее с помощью кредитной карты или сдав в сервисный центр для ремонта, личность нарушителя авторских прав была бы установлена.

Ваши перемещения отслеживаются

Система глобального позиционирования (Global Position Systems, GPSs) улучшила семейную жизнь многих мужчин, которые слишком упрямы, чтобы спрашивать у кого-либо дорогу. Устройство типа «Garmin» или «Tom Tom», установленное в автомобиле, периодически ловит сигналы спутников, отмечающих свое расположение в космосе. Внутренний процессор GPS на основе показаний спутников и времени прохождения сигнала рассчитывает координаты автомобиля. 24 спутника, движущиеся по орбитальным траекториям в 12 500 милях над поверхностью Земли, однозначно определяют координаты объекта

с точностью до 25 футов. Подобное устройство достаточно дешево, чтобы быть популярным подарком ко дню рождения.

В 2004 году Рон Ли арендовал такой автомобиль у компании Payless в Сан-Франциско (штат Калифорния). Мистер Ли проехал на восток, в Лас-Вегас (штат Невада), затем в обратном направлении, в Лос-Анджелес (штат Калифорния), и наконец, вернулся домой. Предполагалось, что поездка обойдется примерно в 150 долларов. Однако компания предъявила счет на 1400 долларов. Как оказалось, мистер Ли не обратил внимания на пункт договора аренды, набранный мелким шрифтом: «Не пересекайте границ штата Калифорния». Пробег автомобиля в пределах Калифорнии арендатором не оплачивался. Но пробег за пределами штата следовало оплатить из расчета 1 доллар за милю. Поскольку на автомобиле находилось оборудование GPS, компания Payless располагала самыми точными сведениями о маршруте клиента.[1]

Оборудование GPS позволяет определить местонахождение приемника в каждой точке земного шара. Альпинисты используют его, потому что оборудование GPS предоставляет трехмерный массив координат, содержащий не только долготу и широту, но и высоту над уровнем моря. Даже обычный мобильный телефон позволяет определить местонахождение владельца. Если телефон находится в зоне покрытия, то он обменивается сигналами с ближайшими базовыми станциями, расположение которых известно. С помощью информации о сигналах можно приближенно установить координаты. Именно так обнаружили миссис Райдер, пострадавшую в аварии (см. главу 1). Точность определения координат невысока (около десятка городских кварталов), но возможность их вычисления так же несомненна, как и то, что фотографии, сделанные цифровой камерой, содержат информацию о месте, времени съемки и идентификационных данных устройства.

Ваша обувь расскажет о своих путешествиях

RFID-метка (Radio Frequency Identification tag, радиочастотный идентификатор) может быть прочитана с дистанции в насколько футов. Это усовершенствованная версия всем знакомого штрих-кода, который обычно используется для установления вида и производителя товара. RFID-метка хранит значительно больше информации. Если конкретный штрих-код может означать что-то вроде «Кока-кола, 0,3 л, алюминиевая банка», то с аналогичной RFID-метки можно считать еще и уникальный идентификационный номер, к примеру: «Кока-кола, алюминиевая банка, № 12345123514002». RFID-данные передаются по радиочастотам, не относящимся к видимому спектру излучения,

[1] Кристофер Эллиот (Christopher Elliot) «Some Rental Cars Are Keeping Tabs on the Drivers» (Машины, взятые напрокат, могут отслеживать маршрут водителя), *New York Times* от 13 января 2004 года.

поэтому при считывании RFID-данных как метка, так и считывающее устройство (ридер) могут быть невидимы.

RFID-метка – это кремниевая микросхема в пластиковом корпусе (чип). RFID-метки можно нанести куда угодно (рис. 2.1). Электронные пропуска представляют собой RFID-метки. При активации в электронном замке с пропуска считывается несколько битов. Карта типа Speedpass компании Mobil является RFID-меткой, исполненной в виде брелока, предназначенного для бесконтактного опознания клиента заправочной станции. Уже около 10 лет домашним животным вживляют RFID-метки для контроля местонахождения. На молочных фермах с помощью RFID-меток ведется учет ежедневных надоев для каждой коровы. Путем идентификации RFID-метки можно установить владельца потерявшегося или украденного животного. Возможность идентифицировать людей при помощи RFID-меток очевидна и давно используется, например, при доступе на объекты атомной энергетики.

Чипы-шпионы

Книга Кэтрин Альбрехт (Katherine Albrecht) и Лиз Макинтайр (Liz McIntyre) с говорящим названием «SPYCHIPS» (Чипы-шпионы), Plume, 2006 содержит множество сведений о действующих и находящихся в разработке RFID-устройствах, используемых производителями и поставщиками потребительских товаров.

Но зачастую RFID-метки применяются для более приземленных целей, например так помечают обувь. Технология RFID может служить основой для любой системы учета и слежения.

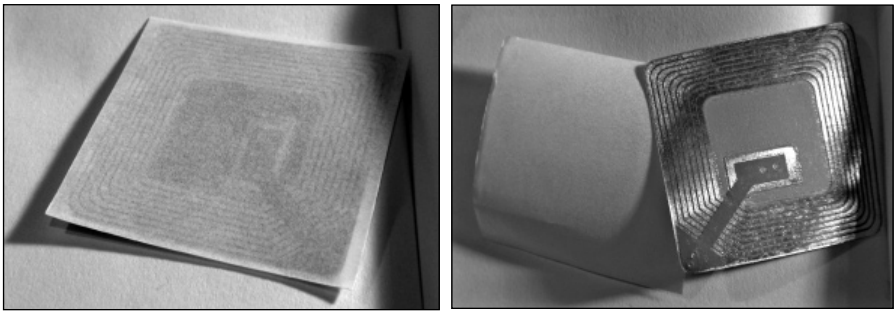


Рис. 2.1. *RFID-метка, обнаруженная между страниц книги. Книжный магазин, получающий партию товара, может проверить содержимое, не прибегая к распаковке. При необходимости можно даже в дальнейшем установить отдел, в котором была куплена книга*

RFID-метки – довольно простые устройства. Они хранят несколько десятков бит информации, обычно уникальной для конкретной области применения. Большинство RFID-меток не имеют источника энергии и невелики по размеру. RFID-метка состоит из микросхемы и антенного элемента, работающего как на прием, так и на передачу. При прохождении через электромагнитное поле (например, через поле ридера, установленного в рамке или под ковром в супермаркете либо находящегося в руке кассира) в антенне индуцируется слабый ток. Этого тока достаточно, чтобы RFID-метка активизировалась и отправила идентифицирующую информацию. Устройство и способ работы меток позволяют легко скрывать их. Часто RFID-метки наклеены на товары; одна такая, показанная на рис. 2.1, была найдена между страниц купленной книги. Некоторые RFID-метки почти невозможно обнаружить.[1]

Обычно технологии RFID используются не для шпионажа, а для удобства хранения записей. Производители и продавцы хотят иметь больше информации и больше надежности, поэтому рады новым технологиям. Не нужно особого ума для того, чтобы представить, во что может вылиться всеобщая электронная инвентаризация. Допустим, вы купили замечательную пару красных туфель (оснащенных RFID-меткой) в Нью-Йоркском универмаге. Если оплата производилась кредитной картой, то универмаг получает информацию о вашем имени и электронный реестр ваших покупок. Месяц спустя вы приезжаете в Лос-Анджелес и, надев новые туфли, заходите в местный универмаг той же компании. Если здесь есть ридер, то не удивляйтесь, когда незнакомый продавец обратится к вам по имени и предложит шарфик, «отлично подходящий» к вашим красным туфлям, или что-то еще, «замечательно дополняющее» одну из ваших прошлых покупок. С другой стороны, из того же источника продавец может узнать о вашей привычке возвращать большинство покупок – и тогда не исключены неожиданные неприятности.

Технологии уже готовы к подобным заданиям. Мы не знаем ни одного магазина, зашедшего так далеко, но в сентябре 2007 года центр Galeria Kaufhof в Эссене (Германия) сделал шаг вперед, установив RFID-ридеры в примерочных кабинках отдела мужской одежды.[2] Когда покупатель примеряет одежду, дисплей на стене показывает доступные размеры и цвета. Система также может предлагать подходящие аксес-

---

[1] *http://www.rfid-asia.info/2007/02/digestible-rfid-tag-alternative-for.htm*. Патентное приложение 20070008113; записано Eastman Kodak Company под названием «System to monitor the ingestion of medicines». Документ описывает «легко переносимый маркер с радиочастотной идентификацией (RFID)».

[2] Риа Уэссел (Rhea Wessel) «Metro Groups Galeria Kaufhof Launches UHF Item-Level Pilot» (Metro Groups Galeria Kaufhof запускает предметный эксперимент с ультракороткими частотами), *RFID Journal* от 20 сентября 2007 года, *www.rdifjournal.com/article/articleview/3624/1/1/*.

суары. Центр хранит записи о примерках и последующих покупках. По просьбе покупателя RFID-метка удаляется из покупки; в ином случае RFID-метки остаются и служат для учета возвращаемых покупок. Творчески настроенные продавцы спят и видят, как подобные технологии помогают зарабатывать еще больше денег и обгонять конкурентов. В данном случае, сеть Galeria Kaufhof не скрывает своих нововведений, однако страх перед тем, что покупателям не понравятся их «гениальные» идеи, часто тормозит решения торговцев или заставляет их действовать скрытно.

«Черные ящики» есть не только в самолетах

12 апреля 2007 года губернатор Нью-Джерси Джон Корзин направлялся в губернаторскую резиденцию в Принстоне, чтобы стать посредником в переговорах одиозного радиоведущего Дона Имуса с баскетбольной командой Университета Рутгерса.

Личный шофер, тридцатичетырехлетний полицейский по имени Роберт Расински, вел автомобиль губернатора по бульвару Гарден Стэйт в северном направлении. Чтобы избежать столкновения с другой машиной, шофер выполнил резкий разворот; по инерции, автомобиль губернатора (модели Chevrolet Suburban) перевернулся. В результате аварии губернатор получил переломы 12 ребер, а также бедра, ключицы и грудины. Подробности происшествия выяснились не сразу. Мистер Расински заявлял, что не помнит, с какой скоростью вел автомобиль.[1] Но вскоре все прояснилось. Губернатор не пристегнул ремень безопасности. Скорость губернаторского автомобиля до аварии составляла 91 милю в час при разрешенной скорости всего 65 миль в час.[2] Рядом с местом аварии не было полицейских с радарами; никто из окружающих не мог точно измерить скорость. Однако, как и еще 30 миллионов американских автомобилей, автомобиль губернатора был оснащен устройством типа EDR (event data recorder, устройство журналирования событий), которое записывало все, что происходило до аварии. Устройство EDR действует подобно «черному ящику» самолета.

Устройства EDR начали устанавливать в автомобили с 1995 года. Согласно федеральному законодательству США с 2011 года установка подобных устройств станет обязательной. Если у вас новая модель GM, Ford, Isuzu, Mazda, Mitsubishi или Subaru, то на ней уже установлено устройство EDR, независимо от того, сообщили ли вам об этом при продаже. Такая же ситуация с половиной автомобилей Toyota. Ваш стра-

---

[1] Алекс Тейлор III (Alex Taylor III) «Corzine crash spotlights SUV Safety» (Авария губернатора Корзина опровергает мнение о безопасности вседорожников), *Fortune* от 19 апреля 2007 года.

[2] Том Хестер-мл. (Tom Hester, Jr. (Associated Press)) «Trooper speeding revealed in Corzine crash» (Причиной аварии автомобиля губернатора Корзина стало превышение скорости), *USA Today* от 18 апреля 2007 года.

ховщик, возможно, получит разрешение воспользоваться записями EDR после возможной аварии.[1] Однако большинство все еще не подозревает о наличии подобных устройств.

Устройства EDR фиксируют состояние датчиков скорости, времени торможения, поворотных сигналов, ремней безопасности – все необходимое для реконструкции хода событий при аварии и установления вины или невиновности.[2] Компания железнодорожных перевозок CSX Railroad не отвечает за гибель водителей, чьи автомобили согласно информации EDR перед моментом столкновения располагались на железнодорожных путях.[3] Полиция обычно (но не всегда) запрашивает разрешение на обыск перед тем, как считать данные EDR. Иногда разрешение не требуется. Когда 18 октября 2003 года Роберт Кристманн сбил пешехода, что привело к смерти последнего, сотрудник полиции штата Нью-Йорк Роберт Фрост получил доступ к данным EDR с автомобиля мистера Кристманна. Из полученных данных следовало, что перед столкновением в зоне с разрешенной скоростью до 30 миль в час автомобиль двигался со скоростью 38 миль в час. Когда данные были представлены суду, мистер Кристманн заявил, что полиция нарушила его права, гарантированные Четвертой поправкой к Конституции США (о запрете произвольных обысков и арестов). Однако суд отклонил это заявление на основании того, что следственные действия, связанные с получением информации EDR, не подпадают под категорию обыска.[4]

Избежать цифровых следов почти так же трудно, как перемещаться, не касаясь земли.

Потоки битов – неотъемлемая часть повседневности. Избежать цифровых следов почти так же трудно, как перемещаться, не касаясь земли. И даже если человек не оставляет следов при ходьбе, он часто неосознанно оставляет отпечатки пальцев.

Иногда вторжение битов в частную жизнь кроется за совершенно безобидными повседневными действиями. Мы уже описали гипотетический случай покупки красных туфель с RFID-меткой, после чего

---

1 Джефф Гэмидж (Jeff Gamage) «Car's 'black box' and what it tells» (Автомобильный «черный ящик», и о чем он может рассказать), *Philadephia Inquirer*, 24 ноября 2007 года. года. Боб Холидей (Bob Holliday) «Little black box: Friend or foe?» (Крошечная черная коробочка: друг или враг?), *The Pantagraph* (Блумингтон, Иллинойс), 4 марта 2007 года.

2 Билл Говард (Bill Howard), «The Black Box: Big Brother's Still Watching» (Черный ящик: Старший Брат все еще наблюдает), *TechnoRide*, 19 апреля 2007 года. *www.technoride.com/2007/04/the_black_box_big_brothers_sti.php*.

3 Лео Кинг (Leo King) «CSX wins wrongful death suit» (CSX выигрывает дело о несправедливом обвинении в причинении смерти), бюллетень *National Corridors*, Vol. 3, № 45, 4 ноября 2002 года. *www.nationalcorridors.org/df/df11042002.shtml*.

4 «Народ штата Нью-Йорк против Роберта Кристманна», суд Нью-Арка, дело 3 Misc. 3d 309; 776 N.Y.S.2d 437, решение вынесено 16 января 2004 года.

покупатель мог при следующем походе в универмаг рассчитывать на радушный прием или враждебность, в зависимости от истории покупок. Похожие сюрпризы могут подстерегать вас почти в любом месте скопления битов. На практике это происходит почти в любой из сфер повседневной жизни.

Следы на бумаге

Отправляя письмо по электронной почте или получая веб-страницу с сайта, я, несомненно, оставляю цифровые следы. Прежде всего, биты должны как-то добраться до меня, поэтому какая-то часть системы знает о моем местонахождении. В старые добрые времена, если хочешь остаться анонимным, можно было написать подметное письмо. Однако при этом был риск оставить отпечатки пальцев на бумаге или быть узнанным по почерку. Можно было напечатать письмо на машинке, однако Перри Мейсон регулярно раскрывает преступления, сравнивая напечатанный текст с уникальным оттиском пишущей машинки предполагаемого преступника. И тут следы.

Сегодня я могу надеть перчатки и напечатать письмо на принтере. Но даже этого недостаточно, чтобы скрыть мою личность. Исследователи из Университета Пэрдью (Purdue) разработали технологию идентификации лазерного принтера по его распечатке.[1] Анализ работы принтера выявил наличие признаков, подобных оттискам пишущей машинки, уникальных для каждого принтера и каждого производителя. Идентифицировать принтер можно даже без микроскопа.

Фонд электронной безопасности (Electronic Frontier Foundation, EFF) демонстрирует, что многие цветные принтеры тайно кодируют заводской номер устройства, дату и время печати на каждой напечатанной странице (рис. 2.2). Так что, печатая донос, не питайте иллюзий насчет того, что никто не сможет узнать имя его автора.

В подобных «сюрпризах» есть определенный смысл. Правительство хочет быть уверенным в том, что офисные принтеры не будут использованы для печати фальшивых банкнот. Такая технология позволяет обнаружить источник подделок. Полезные технологии часто проявляют себя с неожиданной стороны.

Многие желают сохранить анонимность, имея для этого совершенно законные и разумные основания. Это могут быть полицейские осведомители или диссиденты. Или те, кто просто пытается бороться с несправедливостью у себя на работе. Будут ли технологии, позволяющие раскрывать политическую анонимность, использоваться для подавле-

[1] Джон Мелло (John Mello) «Codes Make Printers Stool Pigeons» (Коды печати превращают принтеры в осведомителей), *TechNewsWorld* от 18 октября 2005 года. Веб-страница исследовательской группы университета Пэрдью, *cobweb.ecn.purdue.edu/~prints/index.shtml*.

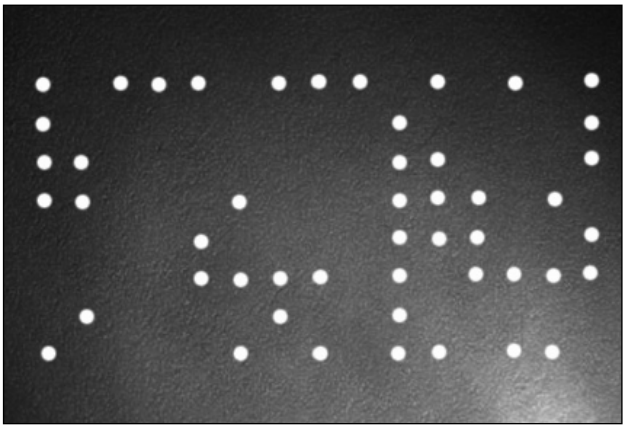


Рис. 2.2. *Лист, напечатанный цветным лазерным принтером Xerox DocuColor 12. Точки почти невозможно увидеть невооруженным глазом; снимок был помещен под источник освещения с чистым синим цветом. Узор из точек содержит дату (21 мая 2005 года), время печати (12:50) и заводской номер принтера (21052857)*

Источник: Лазерный отпечаток пальца. Фонд электронной безопасности, http://w2.eff.org/Privacy/printers/docucolor/

ния свободы мысли? Степень анонимности имеет значение в здоровом демократическом обществе, а в США анонимность была инструментом, способствующим выражению свободы мысли, еще со времен войны за независимость. Остается только сожалеть о полной утрате анонимности ради прелестей технологий связи, применение которых всегда оставляет следы.

Проблема не столько в самом существовании цифровых следов, сколько в том, что никто не говорит нам, как мы эти следы оставляем.

Проблема не столько в самом существовании цифровых следов, сколько в том, что никто не говорит нам, как мы эти следы оставляем.

Автостоянка знает больше, чем вы думаете

Однажды весной 2006 года Энтони и его жена поехали днем встречать друзей в аэропорт Логан на двух автомобилях, по прибытии оставив их на стоянке. Позже, вечером, Энтони и его жена оплатили стоянку в терминале и уехали – вернее, пытались уехать. Автомобиль жены покинул стоянку без проблем, а самому Энтони пришлось задержаться больше чем на час, почти до полуночи. Почему? Потому что его жетон не соответствовал номерному знаку транспортного средства.[1]

[1] Мэтт Дэниел (Matt Daniel) «Starts and Stops» (Старты и остановки), *Boston Globe* от 25 марта 2007 года.

Как выяснилось, у каждого автомобиля, оставляемого на автостоянке аэропорта, при выдаче жетона фотографируется номерной знак. Поскольку Энтони взял два жетона – для себя и для жены, – то ему ничего не стоило их перепутать. Поэтому, когда Энтони попытался выехать, его не пропустили. Нельзя.

Кто бы мог подумать, что два автомобиля, одновременно въехавшие на стоянку, не смогут одновременно выехать? Кто из прибывших мог знать, что номерной знак каждого автомобиля фотографируется?

Этим мерам есть свое объяснение. Водители, набравшие несколько счетов и большую сумму за парковку, иногда пытаются пропихнуть на выходе только один счет, на котором указана самая маленькая сумма. Автоугонщики тоже порой используют этот трюк. Поэтому система учета совершенствуется, решая старые проблемы и создавая новые. Спрашивается, кто еще может иметь доступ к базе номерных знаков? Если полиция разыскивает конкретный автомобиль, может ли она получить доступ к этим данным? Как долго хранятся данные в базе? Сообщает ли вам кто-нибудь, пусть даже мелким шрифтом на чеке, что ваше посещение стоянки не является полностью анонимным?

Вся информация в одном кармане

Рассказ о появлении все новых источников данных – а также о распространении и взаимодействии старых – всего лишь часть истории о цифровом наступлении на частную жизнь. Другая часть истории технологий – то, как все данные собираются вместе.

18 октября 2007 года один из младших сотрудников национальной налоговой службы Великобританиии отправил в правительственный кабинет аудита небольшую посылку посредством частной службы доставки **TNT.** Спустя три недели все еще не доставленная посылка была зачислена в разряд утерянных. Поскольку отправитель не воспользовался сервисом доставки с уведомлением, перемещения посылки невозможно было отследить. Посылку могли неправильно оформить, и тогда она осталась в приемном хранилище, ею могли завладеть преступники.[1]

Известие о произошедшем всколыхнуло нацию. Банки и миллионы частных вкладчиков бросились проверять состояние счетов в поисках возможных хищений. 20 ноября глава налоговой службы подал в отставку. Премьер-министр Гордон Браун обратился к населению с извинениями, а оппозиция обвинила министерство в «неисполнении главного долга – защиты общества».

[1] Эрик Пфаннер (Eric Pfanner) «Britain tries to explain data leak affecting 25 million» (Британия пытается объяснить утечку данных о 25 миллионах граждан), *New York Times* от 22 ноября 2007 года.

В посылке было два компьютерных диска. На дисках была записана база данных с именами, адресами, датами рождения, номерами национального страхования (в США это номера социального страхования) и банковскими счетами 25 миллионов граждан (около 40% населения и почти все несовершеннолетние Великобритании). Налоговой службе понадобились эти данные, потому что большинство несовершеннолетних граждан получает еженедельные правительственные выплаты, а у множества семей есть банковские вклады. Десять лет назад перевезти носители с этими данными можно было только на железнодорожной платформе. Пятьдесят лет назад эти материалы заняли бы целый небоскреб.

Эту катастрофу можно было предотвратить. Было сделано много ошибок, совершенно примитивных. Следовало отправить посылку с уведомлением о вручении. Следовало зашифровать информацию. Не нужно было ждать три недели, прежде чем сообщить о пропаже. Это классические ошибки. Учреждения веками имели дело с пересылкой ценных сведений. Юлий Цезарь использовал шифр, когда требовалось доверить пересылку информации третьим лицам. Что можно было сделать в 2007 году (но не в 1984), так это облечь всю информацию в открытую для чтения, удобную для машинного анализа, умещающуюся в карман форму – и все это «потерять».

Экспоненциальный рост объема носителей, вычислительных мощностей и скорости связи преобразует обычные вещи в нечто совершенно новое. Небрежность, глупость, любопытство, зависть и воровство *не* новы. Тот факт, что данные первостепенной важности о каждом жителе страны могут уместиться в памяти настольного компьютера, – вот *новое*. Возможность «найти иголку в стоге сена» с помощью поисковых систем Интернета – и это *новое*. Легкий доступ к «открытым» источникам тех данных, которые раньше хранились в сейфах и конторских шкафах где-нибудь в Альбукерке или в Атланте, а теперь доступны в электронном виде из Алжира, – тоже нечто совершенно *новое*.

Обучение людей, разработка законов, необходимое программное обеспечение – все это может быть полезно. Но истина в том, что общество совершенно не представляет, как справиться с последствиями цифровой экспансии. Технологическая революция опережает способность общества воспринимать изменения и брать из них только то, что действительно необходимо. Премьер-министру пришлось извиниться перед народом, поскольку битовый взрыв, среди прочего, уничтожил и то положение вещей, при котором ни один министерский чиновник не может нанести нации подобный удар с помощью всего одной небольшой почтовой посылки.

Собирая мозаику

Цифровые следы и отпечатки – только некоторые из новых явлений нашей жизни. Мы уже давно оставляем следы, заполняя налоговые

декларации, бронируя гостиничные номера или звоня по межгороду. Нынешние следы просто более четкие и их легче найти. Но есть еще кое-что – возможности компьютеров сопоставлять данные, прослеживать связи, собирать информацию по кусочкам, создавая четкую, подробную мозаику из казалось бы несвязанных фрагментов. Цифровая экспансия не только сметает и разбивает защитные укрепления личной неприкосновенности. Подобно неумолимо движущемуся весеннему ледоходу, она создает скопления и залежи фрагментов информации. Разберите скопления, разройте залежи, соедините фрагменты – и получится цельная картина.

Компьютеры могут сортировать огромные базы данных, с которыми не под силу справиться людям. Компьютеры способны создавать невообразимые картины из миллионов цветных точек, которые по отдельности ничего не значат. Когда слушалось дело о банкротстве энергетической компании Enron, в руки суда попало около полумиллиона электронных писем. С помощью специальных алгоритмов группировки и построения графов удалось в краткие сроки выявить течения, группы и настроения в среде сотрудников компании на основе только адресов писем (рис. 2.3).[1]

Те же алгоритмы применяются для обработки информации о телефонных звонках. Можно многое узнать о людях только по времени связи и именам адресатов или абонентов. Даже если неизвестно содержание переговоров, можно выстроить цепь причин и следствий, наложив журнал времени связи на историю событий.

При желании можно извлечь многое из общедоступной информации. В штате Массачусетс приобретением медицинских страховок для госслужащих занимается специальное федеральное агентство – Комиссия по групповому страхованию (Group Insurance Commission, GIC). После года работы и выплаты страховых взносов агентство запросило детальную информацию по каждому случаю обращения за медицинской помощью. Для этого была существенная причина: все виды медицинского обслуживания стремительно дорожали. Правительство штата должно отчитываться перед налогоплательщиками в том, куда уходят их деньги. Агентство не требовало имен обратившихся к врачам, не собираясь отслеживать пациентов. Люди не должны думать, что за ними следят. Кроме того, получение информации о содержании визита к врачу противозаконно.

Таким образом, агентство получило базу данных без имен, адресов, номеров социального страхования, телефонных номеров – всего того, что могло бы помочь неподконтрольному руководителю агентства повлиять на определенных людей. Выражаясь на профессиональном жаргоне, данные были «очищены», то есть из них была удалена иденти-

[1] Джеффри Хеер (Jeffrey Heer), курсовой проект по исследованию электронной почты Enron. *jheer.org/enron/v1/*.

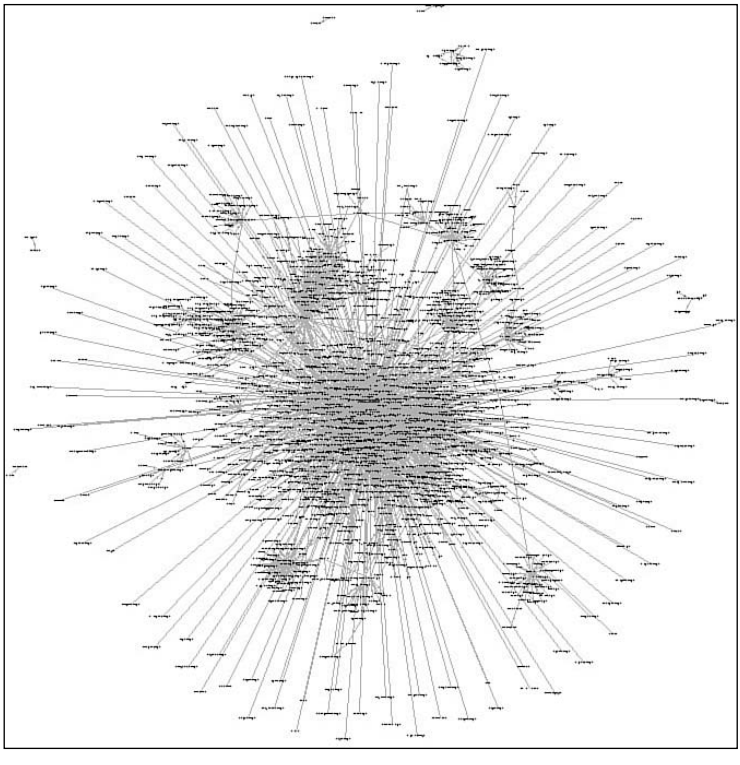


Рис. 2.3. *Диаграмма показывает группы корреспондентов электронной почты компании Enron. Помечены сотрудники, отправляющие особенно много писем. Заметные скопления узлов диаграммы могут свидетельствовать о возможных тайных группировках*

Источник: исследование компании ***Enron, курсовой проект Джеффри Хира (Jeffrey Heer), университет Беркли, Калифорния. Рисунок 3 с веб-страницы*** *http://jheer.org/enron/v1/*

фицирующая информация.[1] Данные содержали пол, дату рождения, почтовый индекс и некоторые другие сведения о тех, кто обращался за медицинской помощью, а также краткое описание причины обращения. Информация была нужна для того, чтобы выявить не определенных людей, а определенные закономерности – например, если дальнобойщики из Уорчестера часто лечатся от заболеваний спины и поясницы, то, возможно, стоит рекомендовать их нанимателям потратиться на спортзалы и тренажеры. Подобный анализ «очищенных» данных проводится и в других штатах.

[1] Прекрасный обзор деидентификации и сопутствующих тем можно найти на веб-сайте лаборатории международной защиты персональных данных Университета Карнеги-Меллона, *privacy.cs.cmu.edu*.

Данные, полученные агентством, представляли ценность не только для него, но и для всех, кого могли интересовать здоровье людей и индустрия здравоохранения в Массачусетсе. Научные сотрудники могли бы использовать такой статистический подарок для эпидемиологических исследований. Агентство заявляло, что, поскольку данные не содержали индивидуальную информацию, их разглашение никому бы не повредило.

Фактически какая-нибудь компания или даже отрасль не отказалась бы приобрести эту статистику. Представьте: агентство продает базу данных (и ее регулярные обновления) медицинской компании. Налогоплательщики получают от этого двойной выигрыш. Во-первых, штат сразу получает новый источник дохода; во-вторых, в долгосрочной перспективе индустрия здравоохранения сможет работать более эффективно.

Но обеспечивали ли данные из базы агентства анонимность на самом деле?

В ожидании должности профессора информатики в университете Карнеги-Меллона Латанья Суини вела исследования в Массачусетском технологическом институте. Она задалась вопросом, насколько сложно восстановить «очищенную» информацию и выяснить состояние здоровья определенного госслужащего, например Уильяма Уэльда, губернатора штата Массачусетс с 1991 по 1997 годы.

Губернатор Уэльд в это время проживал в Кембридже. В этом городе, как и во многих других, регулярно публикуются списки избирателей. Кандидатам и политическим партиям эти списки предоставляются бесплатно; избиратели могут за 75 центов купить списки для своего участка; для всех остальных списки доступны за 15 долларов.

Латанья Суини приобрела списки избирателей для Кембриджа. В списке было шесть человек с такой же датой рождения, как у губернатора, трое из них были мужчинами и только у одного из них почтовый индекс соответствовал адресу губернатора.[1] Полученной комбинации данных – даты рождения, пола и почтового индекса – оказалось достаточно, чтобы сделать из базы данных агентства выборку медицинских записей, относящихся к губернатору и даже к членам его семьи. Личность губернатора была идентифицирована простым подбором ключевых данных. Как выяснилось, в Кембридже по одной только дате рождения можно идентифицировать 10% проживающих. В масштабе

[1] Латанья Суини (Latanya Sweeny) «Recommendations to Identify and Combat Privacy Problems in the Commonwealth» (Рекомендации по идентификации и борьбе с проблемами нарушения права на неприкосновенность частной жизни населения штата), выступление перед выборным комитетом штата Пенсильвания по информационной безопасности (резолюция № 351), Питтсбург (штат Пенсильвания), 5 октября 2005 года, *privacy.cs.cmu.edu/dataprivacy/talks/Flick-05-10.html*.

всей страны с помощью вышеупомянутой комбинации данных можно идентифицировать 87% населения.[1]

Но база данных агентства содержала гораздо больше ключевых данных. Фактически все люди, чьи данные содержались в базе, – 135 тысяч человек – могли быть идентифицированы любым из 58 покупателей базы 1997 года. «Врачебной тайны больше не существует, – заявил доктор Джозеф Хейман, президент Массачусетского медицинского общества (Massachusetts Medical Society). – Она утрачена».[2]

Казалось бы, в такой истории должны были «полететь головы». Но на самом деле чрезвычайно трудно выяснить, кто допустил ошибку, если она была. В сущности, нет ничего плохого в сборе информации с целью способствовать снижению всеобщих расходов на здравоохранение. Агентство действительно попыталось «очистить» данные, обеспечив анонимность граждан. Можно сказать, что агентство не должно было передавать базу данных другим отделам правительства или в третьи руки, но этот аргумент сродни предложению завести для каждого отдела в здании правительства собственную котельную. Информация является критическим ресурсом, и правительство совершенно право в стремлении направлять ее распространение только во благо общества. Можно критиковать агентство за сам факт продажи информации, но это несущественный аргумент: поскольку предполагалось, что данные обеспечивали анонимность, трудно упрекнуть кого-либо в чрезмерном стремлении снизить расходы налогоплательщиков на содержание правительственного аппарата.

Казалось бы, в такой истории должны были «полететь головы». Но на самом деле чрезвычайно трудно выяснить, кто допустил ошибку, если она была.

Возможно, ошибка заключалась в свободном распространении списков избирателей. Но это традиция, и открытые выборы – неотъемлемая часть избирательной системы. Общественность вправе знать, кто вправе избирать и кто сделал выбор. Кроме того, списки избирателей не единственный источник данных о населении США. Если вас вдруг заинтересует количество уроженцев Гавайских островов в возрасте 21 года, проживающих в округе Мидлсекс штата Массачусетс в 2000 году, то из данных всеобщей переписи населения можно узнать, что их четверо. Данные всеобщей переписи доступны всем желающим

---

[1] Латанья Суини (Latanya Sweeny) «Comment of the Department of Health and Human Services on “Standards of Privacy of Individually Identifiable Health Information“» (Комментарии департамента здравоохранения и социального обеспечения к «Стандартам безопасности персональной медицинской информации»), *privacy.cs.cmu.edu/dataprivacy/HIPAA/HIPAAcomments.html*.

[2] Майкл Ласаландра (Michael Lasalandra) «Panel told releases of med records hurt privacy» (Медицинская общественность заявила, что раскрытие медицинской информации нарушает право на неприкосновенность частной жизни), *Boston Herald* от 20 марта 1997 года.

восполнить недостающие фрагменты в портрете чьей-то личности (*factfinder.census.gov*).

Ошибкой было считать, что данные в базе агентства действительно обеспечивают анонимность. Множество доступных источников информации вкупе с огромной вычислительной мощью современных компьютеров и эффективными алгоритмами нахождения связей заставляют урезать ключевые данные еще больше. Объединение данных (например, пятизначные почтовые индексы менее информативны, чем девятизначные) может существенно усложнить вычисления. Однако слишком усердная «очистка» баз данных может в конце концов сделать их бесполезными для первоначальных целей.

Большую проблему можно попробовать решить, разделив ее на множество проблемных компонентов, решаемых по отдельности. Но как можно решить проблему, состоящую из компонентов, каждый из которых сам по себе проблемным не является?

Почему мы утратили (или просто отбросили) право на неприкосновенность частной жизни

Информационные технологии не больше ответственны за потерю неприкосновенности частной жизни, чем рост автопрома за подростковый секс. Технологии несут в себе как риски, так и перспективы, а люди (как личности и как члены общества) сами решают, как им жить в новом мире. Чтобы осознать, что мы потеряли, придется обратить внимание не только на мобильные устройства. Надо остерегаться шпионов и мошенников, но надо и помнить о тех, кто в новом мире помогает нам и обеспечивает нашу защиту,– и не забывать о том, что порой виновник смотрит на нас из зеркала.

Обычно мы задумываемся об утечке персональных данных, только когда эти данные оказываются утеряны или украдены. События, подобные случившимся в налоговом ведомстве Великобритании, не столь редки. Потери, связанные с кражей информации о 45 миллионах клиентах сетевого ритейлера TJX (подробнее в главе 5), превышали масштаб британской катастрофы. В 2003 году Скотт Левин, владелец сервиса массовой рассылки Snipermail, украл больше миллиарда персональных записей у компании маркетинговых консультаций Acxiom.[1] Миллионы американцев ежегодно становятся жертвами кражи персональных данных, терпя убытки на десятки миллиардов.[2] Еще больше

[1] Джалкумар Виджаян (Jalkumar Vijayan) «Appeals Court: Stiff prison sentence in Acxiom data theft case stands» (Апелляционный суд назначил срок за кражу данных Acxiom), *ComputerWorld* от 23 февраля 2007 года.

[2] «Javelin Strategy & Research». Отчет об исследованиях случаев подделки идентификации, февраль 2007 года, *www.privacyrights.org/ar/idtheftsurveys.htm*.

людей постоянно опасаются очередной кражи порции битов финансовой информации и возможного крушения своего благополучия.

Почему мы не можем держать личную информацию при себе? Почему многие люди хранят важные сведения на виду, так что они просто обречены потеряться или спровоцировать умелых мошенников на кражу?

Мы потеряли контроль над персональной информацией благодаря собственным поступкам и действиям окружающих по отношению к нам. Мы теряем контроль, когда стараемся идти в ногу со временем или хотим быть похожим на других. Мы теряем контроль, когда жертвуем им ради экономии денег или времени. Мы теряем контроль, пытаясь защититься от врагов или чувствуя безнаказанность. Нет единого решения проблемы потери персональной информации и неприкосновенности частной жизни, потому что нет единой причины, порождающей эту проблему. Чтобы найти решение для себя, каждый должен сесть и обдумать свои действия.

Мы раздаем персональную информацию, беспечно оставляя четкие цифровые следы на дороге нашей жизни, решив (возможно, без долгих раздумий), что преимущества цифровых технологий перевешивают недостатки. Честно говоря, преимуществ действительно много.

Экономия времени

Те, кто пользуется платными автострадами, часто даже не замечают недостатков цифровых технологий. Время – деньги, а время в автомобильной пробке – это вдобавок утомление и головная боль. Если есть возможность приобрести электронный пропуск на автостраду, большинство водителей это сделают, даже если за сам пропуск надо доплатить. Вид из окна собственного автомобиля на вереницу других, чьи водители вынуждены тратить время на оплату, – это не только смена пейзажа, но еще и картина, вызывающая ощущение собственного превосходства.

Пропуск, прикрепляемый изнутри к ветровому стеклу, – не что иное, как RFID-метка с батарейкой, отправляющая сигнал ридеру, когда автомобиль пролетает мимо него. Ридер может быть установлен на месте, где обычно располагается кабинка контролера. Или на арке прямо над дорогой, так что водителю даже не нужно менять полосу или снижать скорость.

Где же здесь недостатки? Конечно, ведется журнал каждого пересечения меткой границы платной автострады; таким образом, ведется учет расходов на проезд. Когда баланс пропуска снижается до критического уровня, можно автоматически перевести средства с кредитки водителя. Все это только добавляет удобства – не нужно возиться со сдачей и вообще доставать кошелек, чтобы оплатить скорый проезд.

Ежемесячный счет, например для автострады Фаст Лейн в Массачусетсе, содержит точные (до секунд) сведения о том, где и когда водитель

въехал на автостраду. Также счет содержит данные о времени выезда с автострады и пробег. Сведения о пробеге – полезный сервис, так как водитель иногда может вернуть часть суммы, потраченной на заправку в пределах автострады. И школьник догадается, что по этим данным компьютер может в два действия рассчитать среднюю скорость движения автомобиля. Технически несложно добавить к ежемесячному счету еще и сумму штрафа за возможное превышение скорости, при необходимости списав нужную сумму с кредитной карты. А вот это уже не очень похоже на удобство; впрочем, пока что ни в одном штате до такого не додумались.

Зато додумались использовать электронные журналы пользования платными путями в бракоразводных процессах и делах об опекунстве. «Что? Вы никогда не приближались к дому этой дамы ближе, чем на пять миль? Правда? Тогда почему вы многократно выезжали с автострады рядом с вышеупомянутым домом?» Попытки доказать, что некто сможет лучше заботиться о детях, часто опровергаются фактами. Как сказал один адвокат, если муж говорит: «Да я каждый день возвращаюсь домой около пяти и ужинаю вместе с детьми», запросите в судебном порядке журнал пользования платным мостом и выясните, в котором часу этот тип каждый вечер его пересекает (хе-хе). Случаи запросов журналов пользования платными путями при рассмотрении семейных дел исчисляются сотнями. Часты такие запросы и в делах с участием работника и нанимателя, когда требуется доказать, что машина работника в неположенное время была далеко от предполагаемого места работы.[1]

И все же большинство из нас не собирается надувать супруга или начальство, так что утрата неприкосновенности частной жизни вовсе не представляется таковой, по крайней мере, в сравнении с сэкономленным временем. Конечно, если бы мы на самом деле *обманывали*, то при крайней спешке, *возможно*, ради экономии нескольких минут и рисковали бы потерять что-то гораздо более существенное.

Экономия денег

Иногда к утрате индивидуальности нас побуждает стремление сэкономить деньги. Явный пример – дисконтные карты в супермаркетах. Если вы не хотите, чтобы торговая сеть Safeway сохранила запись

[1] Дэниел Б. Вуд (Daniel B. Wood) «Radio ID tags proliferate, stirring privacy debate» (Число радиочипов увеличивается, вызывая споры о нарушении права на неприкосновенность частной жизни), *Christian Science Monitor* от 15 декабря 2004 года; Дебби Хоулет (Debbie Howlett) «Motorists can keep on rolling soon» (Автолюбителям вскоре облегчат жизнь), *USA Today* от 26 мая 2004 года; «High-Tech Evidence, A lawyer's friend or foe?» (Высокотехнологичные улики – друзья или враги юристов?), *National Law Journal* от 24 августа 2004 года.

о том, что несмотря на результаты недавней проверки уровня холестерина вы все-таки купили 12 кексов Yodels, то у вас есть эта возможность. Вам всего лишь придется выложить «плату за приватность» – надбавку к цене для покупателей, не имеющих дисконтной карты. Эти карты позволяют продвцу фиксировать индивидуальные покупки. (Компании, выпускающие кредитные карты, обычно не интересуются тем, купили вы жирные кексы или диетические хлопья, поэтому не регистрируют отдельные мелкие транзакции.) По журналу ваших покупок по дисконтной карте торговая сеть может выстроить зависимость ваших покупок от ваших привычек. Затем, если выяснится, что покупатели кексов берут в придачу пиво Bison Brew, касса может автоматически делать скидку на пиво при совместной покупке. Покупателям – скидка, супермаркету – повышение объемов продаж. Все выигрывают. Вроде бы все.

По мере роста доли ее бизнеса в Интернете компании Safeway становится легче накапливать персональную информацию. Чтение части пользовательского соглашения, обычно набранной мелким шрифтом, – досадная, но все же необходимость. Можно узнать много нового о том, что вы даете компании и что получаете. Вот несколько фраз из заявления о политике неразглашения информации по отношению к пользователям веб-сайта компании Safeway:

> Safeway может использовать Вашу персональную информацию для того, чтобы обеспечивать Вас новостями, статьями, предупреждениями относительно продуктов или услуг, анонсами продуктов или услуг, призовыми скидками, приглашениями, особыми талонами, программной или рекламной информацией, которая может быть предоставлена Safeway другой компанией... Safeway может предоставлять персональную информацию своим партнерам и поставщикам с целью поддержки клиентов и использования персональной информации в интересах Safeway. Также возможно распространение персональной информации аффилированным компаниям или в случае действительной или возможной продажи, реорганизации, объединения, слияния или поглощения бизнеса Safeway.

Это монотонное чтиво показывает, сколько поблажек делает себе компания. Возможно, вас не особенно донимает спам. Кто-то не считает письма компании спамом; компания даже предоставляет возможность выбирать, какие письма получать, а какие нет, хотя этим мало кто пользуется. Далее, у компании Safeway есть множество «аффилированных компаний», и кто знает, сколько еще «партнеров» может участвовать в сделках по продаже или слиянию с бизнесом Safeway. Несмотря на явные предупреждения, распространяемые сообществами вроде C.A.S.P.I.A.N (Противодействие покупателей действиям супермаркетов по вторжению в частную жизнь и оцифровыванию, Consumers Against Supermarket Privacy Invasion and Numbering, *www.nocards.org*), большинство покупателей готовы дать согласие на сбор персональных данных. Трудно противостоять наживке из скидок и промо-акций.

Но после того как вы проглотите наживку, в базе данных продавца появляется запись с вашим именем, которая со временем пополняется новыми данными, например: пользуетесь вы обычными или увеличенными тампонами, покупаете презервативы со смазкой или без, предпочитаете классическое или легкое пиво. Вы сами предоставили компании право поделиться этими сведениями, которые могут быть проданы, потеряны, украдены или запрошены судебными органами.

Ради удобства покупателей

Самый серьезный аргумент против беспокойства об утечке персональных данных состоит в том, что у покупателя бизнес с компанией, и улучшать этот бизнес – в интересах самого покупателя. Вам нет дела до того, что компания обогащается за ваш счет, но вы серьезно заинтересованы в более быстром и качественном обслуживании и исчезновении не нужных вам товаров. Поэтому заинтересованы обе стороны. В заявлении о политике неразглашения информации компании Safeway сказано: «Информация о карте Клуба Safeway и другая информация может быть использована в целях улучшения продуктов, услуг и программ Safeway ради удобства покупателей». Четко и ясно.

Нет компании, добившейся бóльших успехов в предложении покупателям наиболее привлекательных товаров, чем онлайн-магазин Amazon. Их компьютеры анализируют журналы не только покупок, но и просмотров описаний товаров, так что, зайдя на сайт Amazon во второй раз, посетитель может увидеть специально и индивидуально рекомендованный список товаров. Алгоритмы анализа не совершенны, но чем чаще вы посещаете сайт Amazon, тем меньше ошибок в рекомендательных списках. Если вам не нравится Amazon, зайдите на сайт магазина Barnes & Noble. Снова тот же вопрос: стоит ли беспокоиться, что Amazon может узнать о тебе так много? На первый взгляд, ответ прост. Беспокоиться надо только о том, чтобы кто-то другой не узнал данные твоей кредитной карты. Но кого интересует, какие книги ты предпочитаешь?

Подобное безразличие – еще одно свойство нашей жизни в оцифрованном мире. Когда в 1988 году работник пункта видеопроката передал репортеру газеты «Вашингтон Пост» список фильмов, которые брал судья Роберт Борк, обнародование этого списка способствовало решению Сената отказать судье Борку в праве занять должность члена Верховного Суда. Более того, Конгресс с невиданной скоростью принял довольно жесткий Акт о защите персональной информации при использовании видеопродукции (Video Privacy Protection Act).[1] Пункты видеопроката, если они еще есть, могут быть оштрафованы уже за то, что слишком долго хранят записи о клиентах. Двадцать лет спустя почти никого уже не интересует, что Amazon делает со своими миллионами подробных записей о предпочтениях клиентов.

[1] Кодекс законов США, том 18, раздел 2710, 1988 год.

Как веб-сайты узнают вас

1. **Вы сами им сообщаете.** Введите имя и пароль для входа на Gmail, Amazon или eBay – и они вас узнают.
2. **Сайты оставляют в cookies информацию о ваших прежних визитах.** *Cookie* – это небольшой текстовый файл, сохраняемый на диске вашего компьютера и содержащий информацию о том, что сайту требуется от вас в течение текущего (например, содержимое «корзины для покупок») или следующего сеанса. Для сайта файлы cookies – постоянный источник информации для опознания и отслеживания. Просмотрите список файлов cookies с помощью соответствующей команды вашего броузера, и вы удивитесь, как много сайтов их оставляют.
3. **Сайты видят ваш IP-адрес.** Чтобы отправить запрошенную страницу, программное обеспечение веб-сервера должно знать ваш IP-адрес. IP-адрес – это числовой код вроде 66.82.9.88, уникально определяющий каждый компьютер в Интернете (подробности в Приложении). IP-адрес часто бывает динамическим, но ваш интернет-провайдер в любом случае знает, кому и когда IP-адрес был присвоен. Журналы провайдера нередко попадают на столы судей.

Чтобы узнать, кто использует конкретный IP-адрес, можно обратиться в Американский реестр адресов Интернета (American Registry of Internet Numbers, *www.arin.net*). Сервисы *whatismyip.com*, *whatismyip.org* и *ipchicken.com* также позволяют вам проверить свой IP-адрес. Сервис *www.whois.net* поможет узнать, кто является владельцем доменного имени: к примеру, сайт *harvard.com* принадлежит частному книжному магазину Harvard Bookstore – прямо напротив университета. К сожалению, эта информация не избавит вас от спамеров, так как те часто подменяют имя источника спама.

Разоблачаться – это просто забавно

Иногда невозможно объяснить желание человека открыть свои личные тайны ничем, кроме удовольствия от самого акта публичного обнажения. Эксгибиционизм явление не новое. И сегодня, и в прошлом к публичному разглашению личных тайн чаще склонны либо молодые, либо пьяные, либо те, кто пытается хотя бы так привлечь к себе внимание. Из этого правила, конечно, есть исключения. Ректор университета была вынуждена принести извинения, когда с ее страницы в MySpace в Интернет «просочилась» фотография, где она угрожала

стеком некоему латиноамериканцу, с подписью «бью мексиканцев за то, что постоянно заигрывают с моей дочерью».[1]

В Сети полно непристойностей. Тут и групповые фотографии (их меньше), и множество отдельных фотографий из блогов, где блоггеры в основном делятся своими чувствами. Не столько из распущенности, сколько из обычного стремления избавиться от одиночества. В этом тоже нет ничего нового. *Действительно* новое – то, что фотография, видео или запись в дневнике, стоит их опубликовать, сразу и необратимо становятся доступны всему миру. Биты не стареют и не изнашиваются. Биты вечны. И неясно, как с этим быть.

Биты не стареют и не изнашиваются. Биты вечны. И неясно, как с этим быть.

Вот характерный образчик блога:[2]

> Это персональный сайт Сары МакОли... Я думаю, что делить свою жизнь с незнакомыми – это странность и самолюбование, но мне это нравится, и я веду блог уже несколько лет. Хотите еще? Можете посмотреть страницу «Обо мне», скинуть мне е-мейл или просто почитайте мою ежедневную болтовню.

Спасибо, как-нибудь в другой раз. Другой пример: в Facebook есть группа специально для женщин, которые хотят выкладывать свои фотографии, где они пьяны в стельку.[3] Или вспомните Jennicam, где Дженнифер Кэй Рингли транслировала свою жизнь в течение нескольких лет. Этот «подвиг», во всей его утрированной обыденности, повторяли и пытались «превзойти» многие. Мы обожаем экспериментировать, как актеры и как зрители.

Потому что иначе никак

В конце концов, мы теряем право на неприкосновенность частной жизни просто потому, что нам не хватает времени, терпения или силы воли, чтобы жить иначе. В США миллиарды кредитных, дебетных и банковских карт. Каждый раз при их использовании фиксируются несколько битов информации о том, кто, где, когда и для чего воспользовался картой. Сегодня почти не встретишь тех, кто делает крупные покупки за наличные. Банковские чеки вслед за магнитной лентой уступают место новым технологиям. Даже если вы будете оплачивать наличными каждую покупку, все ваши шаги станут известны налого-

---

1 «Salisbury U. president removes Facebook profile after questions» (Неудобные вопросы привели к тому, что ректор университета Сэлисбери удалила свой блог в Facebook), *Associated Press* от 17 октября 2007 года.

2 *www.smokeandashes.net*

3 Эндрю Леви (Andrew Levy) «The ladettes who glorify their shameful drunken antics on Facebook» (Девицы выставляют свои пьяные кривлянья в Facebook), *Daily Mail* от 5 ноября 2007 года.

вой службе. Известны попытки внедрения RFID-меток в банкноты для отслеживания перемещения денег.

Только секты вроде амишей могут пока обходиться без электричества. Скоро будет практически невозможно обойтись без Интернета со всеми цифровыми следами, оставляемыми вами при регистрации на сайтах, в журналах загрузок и запросах к поисковым системам. Даже старое доброе эфирное телевидение уступает место цифровому. Видеопередачи по Интернету доступны в любое время – не нужно идти в пункт проката или ждать почтовой доставки, потому что ваш заказ примет и обработает телевизионный сервис-провайдер. Ради возможности смотреть все, что захочется, в любое время люди забудут свободу тех дней, когда источником звука и изображения была телевышка, рассылающая радиоволны всем подряд. Время вещания нельзя было выбрать, зато никто не знал, на какую волну вы настроены.

Младший Брат смотрит на тебя

Итак, мы рассмотрели, как к потере права на неприкосновенность частной жизни приводят наши собственные действия. Действительно, можно обойтись без дисконтных карт, внимательно читать договоры и так далее. Самое лучшее – собрать волю в кулак, быть бдительным и говорить решительное «нет» всем похитителям личной информации, но на это способны немногие. Даже тех, кто способен и готов к этому, ждут проблемы, вызванные действиями других.

Любопытный сосед – классический персонаж американских комедий. Он вечно пытается что-то выяснить – сколько пивных бутылок в вашем мусорном баке, чей «мерседес» регулярно паркуется у вашего подъезда, чьи это дети хулиганили ночью в прошлую субботу. В киберпространстве мы все – соседи. И можем «подсматривать» друг за другом в «окна», распахнутые настежь.

Публичные документы становятся общедоступными

Раньше, чтобы сунуть нос в чужие дела, можно было пойти в городскую ратушу и оплатить запрос в местный архив или иное учреждение. Сведения, которые тогда были публичными – но не общедоступными,– теперь реально общедоступны.

В 1975 году Конгресс создал Федеральную избирательную комиссию (Federal Election Commission), чтобы следить за исполнением Акта о федеральной избирательной кампании (Federal Election Campaign Act). С этого момента информация обо всех взносах в поддержку избирательной компании стала публичной. Однако есть существенное различие между словами «публичный» и «общедоступный». Публичные данные, размещенные в Интернете, становятся действительно общедоступными без каких-либо бюрократических препятствий.

Хотите узнать, кто оказал сенатору Элу Франкену финансовую поддержку? Это Лорн Майклс из комедийного шоу «Saturday Night Live», актер, режиссер и поэт Леонард Нимой, спортсмен и обладатель «Оскара» за лучшую мужскую роль Пол Ньюмен, Крейг Ньюмарк (создатель сервиса рассылки объявлений *craigslist.com*) и Джинни У., наша сотрудница, которая не хочет, чтобы мы узнали о ее политических предпочтениях. Наши друзья Пол Б. и Генри Г. поддержали и Обаму, и Хилари Клинтон.

Действие акта направлено на выявление дарителей очень крупных сумм. Но раз регистрации подвергаются все подряд, так почему бы нам не проверить и соседей? Наши определенно склоняются на сторону Обамы, а о существовании кандидата Хаккаби и вовсе никто не вспомнил. Проверим клиентов? Один из них явно поддерживает Денниса Кучинича. А как насчет дружка дочери? Это вы и сами можете узнать на *www.fec.gov* или *fundrace.huffingtonpost.com*. О своих политических предпочтениях мы, пожалуй, промолчим.

В Интернете теперь можно отыскать и другую полезную информацию, например такую, за которой раньше пришлось бы обратиться в бюро по регистрации сделок с недвижимостью. Не составит особого труда узнать, например, сколько ваш сосед платит за свой участок или сколько стоит сегодня его дом. Эта информация всегда была «публичной» – теперь она общедоступна. Эту информацию всегда можно было получить законным путем – но сегодня это делается быстрее и проще.

Сведения об интересующей вас личности часто можно отыскать в социальных сетях (Facebook, MySpace) или с помощью той же поисковой системы. «Ваш колледж, конечно, не интересует дурацкая персональная страница абитуриента на Facebook?» – «Разумеется, нет, – отвечает глава приемной комиссии. – Если, конечно, никто не сообщит, что на ней можно найти нечто любопытное».[1]

Новые сайты со специфическими темами в предоставлении информации заходят еще дальше. Если вы собираетесь встретиться с малознакомым человеком, вам может пригодиться сайт *www.dontdatehimgirl.com*. Когда авторы посетили сайт, там только что появилось новое объявление, сопровождаемое именем и фотографией: «Жуткий бабник, лжец, злостный интернет-читер; патологический обманщик, которому нельзя доверять ни как другу, ни тем более как близкому человеку. Бессовестный подхалим! У него „едет крыша“, ему нужен психолог. Держите вашу дочь подальше от этого парня!» Такая информация заслуживает хорошей оплаты. Учет опасных водителей ведется на сайте *www.platewire.com*. Если вас интересуют нынешние или потенциальные соседи или вы сами хотите предупредить других обывателей,

[1] Рэйчел Арндт (Rachel Arndt) «Admissions officers poke around Facebook» (Сотрудники приемной комиссии шарят в Facebook), *Brown Daily Herald* от 10 сентября 2007 года.

добро пожаловать на сайт *www.rottenneighbor.com*. Когда мы зашли на сайт и ввели почтовый индекс дома одного из авторов, то увидели карту Google, на которой одно из зданий было отмечено красным. После щелчка на нем всплыло следующее сообщение:

> ты хорошенькая блондинка, стройная и яркая. я бы приударил за тобой, но я гей. наверное, тебе, как большинству красавиц, улыбается весь мир. и ты думаешь, что слишком хороша для того, чтобы убирать за своей собакой. ты знаешь, что нарушаешь закон и выказываешь неуважение к соседям? что ж, желаю тебе самой наступить в то, что ты не убираешь, по пути на работу или домой. надеюсь, аромат твоего чувства собственной важности будет сопровождать тебя весь день.

Немного потратившись, вы можете получить еще больше сведений. В январе 2006 года создатель сервиса блогов *Americablog.com* Джон Аравозис приобрел детальный список телефонных звонков генерала Уэсли Кларка.[1] Листинг, содержащий историю звонков за 3 дня, стоил примерно 90 долларов. Подобные услуги предлагаются на десятках сайтов. Как видите, не нужно работать в полиции или ФБР, чтобы узнать, кто, кому и как часто звонит. Спрос на информацию породил соответствующее предложение – и за вполне умеренную плату. Газета *Chicago Sun Times* решила проверить достоверность предоставляемой информации, предложив владельцам сервиса *locatecell.com* достать месячный листинг телефонных звонков Фрэнка Мэйна, одного из репортеров газеты, за 110 долларов. Заказ был сделан в пятницу и содержал номер телефона, временной отрезок и номер кредитной карты. Во вторник по электронной почте пришел ответ. Листинг содержал 78 номеров, по которым звонил репортер: источники из правоохранительных органов, герои репортажей, редакторы – все они были в этом листинге. Такой сервис был бы хорошим подспорьем для полиции, если не считать того, что он в равной степени доступен и преступникам.[2] Рождение сервисов получения списков телефонных звонков привело к созданию Акта о неприкосновенности информации, относящейся к телефонным переговорам (Telephone Records and Privacy Act). Акт был принят в 2006 году, но и в начале 2008 года сервис *locatecell.com* все еще предлагал свои услуги.

Если вам все еще недостаточно информации, можно углубить наше расследование. За 175 долларов вы зарегистрируетесь в сервисе ChoicePoint как «наниматель» и получите доступ к самой разнообразной статистике: криминальные сводки; кредитная история; регистрация транспортных средств; списки учащихся или сотрудников; статистика Интерпола; регистрация преступлений против половой неприкос-

---

[1] *www.americablog.com/2006/01/americablog-just-bought-general-wesley.html*

[2] Фрэнк Мэйн (Frank Main) «Everyone can buy cell phone records» (Журналы сотовых операторов может купить любой желающий), *Chicago Sun-Times* от 5 января 2006 года.

новенности; списки лиц, находящихся в розыске. Прейскурант *для оплаты кредиткой* прилагается. Когда у нас была бумага, но не было битов, эта информация была «публичной», но, как правило, была доступна только профессионалам или ограниченному кругу сотрудников. Теперь все, что нужно для доступа к ней, – подключение к Интернету и кредитка. Это одна из самых важных трансформаций права на неприкосновенность частной жизни.

Программы для мониторинга действий пользователей (personal computer monitoring software)

Программа PC Pandora (*www.pcpandora.com*) позволяет вам «знать все, что пользователи делают на своем ПК», включая «тайные учетные записи электронной почты, онлайн-общение с неизвестными собеседниками, секретные профили данных и личные записи». Вы можете «получить сведения о паролях к почтовым ящикам, собеседниках, регистрациях на сайтах и многое другое».

Программа Actual Spy (*www.actualspy.com*) – кейлоггер (программа, ведущая журнал нажатий клавиш), позволяющий «узнать, что другие люди делают на вашем компьютере в ваше отсутствие. Программа разработана для скрытого мониторинга пользовательской активности. Actual Spy может записывать все нажатия клавиш, сохранять снимки экрана и буфера обмена, вести историю запуска и завершения приложений».

А вот немного настоящего шпионажа. Беверли О'Брайен заподозрила, что муж ей изменяет, ища знакомства на стороне, если не в реальности, то, по крайней мере, в Интернете. Поэтому миссис О'Брайен установила на семейном компьютере программу для мониторинга действий пользователей. Обычно такие программы рекламируются как «средства родительского контроля» («parental control software»), но ими не брезгуют ни работодатели, ни правоохранительные органы, ни ревнивые супруги. Просмотрев журналы программы, миссис О'Брайен выяснила, что ее злополучный муженек вел оживленную переписку, играя в домино на сервисе Yahoo! Dominoes. Это уже был настоящий шпионаж, этакая «домашняя прослушка». Между прочим, поставщики программы «забыли» упомянуть в описании, что применение подобного программного обеспечения является перехватом линии связи и нарушает Акт о безопасности коммуникаций штата Флорида. Поэтому суд отказался рассматривать журналы программы в качестве доказательства факта измены на бракоразводном процессе супругов

О'Брайен.[1] Однако независимо от поведения судебной системы подобный шпионаж – нередкое явление в отношениях между неверными супругами или любовниками, работодателями и работниками, а также конкурентами.

Праздное любопытство

Есть еще одна разновидность «синдрома Младшего Брата», когда некий доморощенный аналитик может, сидя в Интернете, просто наблюдает за тем, что попадется на глаза. Из безбрежного моря данных любой способен без труда выловить интересные факты. Представим, что имена и историю обращений вашей семьи к врачам можно выудить из статьи в онлайн-издании медицинского журнала.

На рис. 2.4 показана карта вспышек болезни, скажем сифилиса, в районе Бостона. «Эпидемия сифилиса» на этой иллюстрации смоделирована. Данные произвольные, но подобные карты десятилетиями фигурируют в медицинских изданиях. Поскольку карта покрывает больше 10 квадратных километров, можно выделить только кварталы, но не отдельные дома.

Так было в те времена, когда выходили только бумажные журналы. Онлайн-издания помещают в Интернет изображения в формате JPEG с высоким разрешением. На рис. 2.5 показан результат наложения части скачанной карты на соответствующую схему городских кварталов. Четко видно, что каждому очагу заболевания соответствует единственный дом. Таким образом, любой человек может выяснить, где проживают зараженные сифилисом.

Перед нами такой же случай восстановления «очищенных данных», как и в исследовании Латаньи Суини, которая показала метод реконструкции медицинской истории губернатора Уэльда. Снова возникает вопрос, как предотвратить реконструкцию. Возможно, не следует использовать карты такого высокого разрешения (хотя может потеряться их наглядность и масштабируемость – одно из преимуществ онлайн-изданий). Возможно, следует «размыть» детали изображения. Для каждого конкретного случая возможной реконструкции данных необходимо выбрать свое решение, и это затрудняет вывод общих правил для «очистки» публикуемой информации.

В 2001 году четыре студента Массачусетского технологического института в курсовом проекте реконструировали данные о жертвах убийств в Чикаго. Ресурсы были крайне ограничены: никаких закрытых или фирменных баз данных; нет доступа к государственным архивам; скудные вычислительные мощности. Даже в таких условиях

[1] Дело «О'Брайен против О'Брайена», № 5D03-3484 (окружной апелляционный суд штата Флорида, 11 февраля 2005 года), *www.5dca.org/Opinions/Opin2005/020705/5D03-3484.pdf*.

Рис. 2.4. *Карта части Бостона, подобная публикуемым в медицинских журналах, с указанием очагов заболевания (вымышленные данные)*

Источник: Джон С. Бронштейн, Кристофер А. Кэсса, Кеннет Д. Мэндл «No place to hide – reverse identification of patients from published maps» (Невозможно спрятаться – раскрытие врачебной тайны с помощью карт эпидемий), New England Journal of Medicine, 355 (16) от 19 октября 2007, с. 1741–1742

Рис. 2.5. *Наложение части изображения с рис. 2.4 на соответствующую схему городских кварталов (увеличено). Каждый, кто имеет доступ к онлайн-версии карты эпидемии высокого разрешения, может выделить отдельные дома*

студенты реконструировали личности 8 тысяч жертв из предполагаемых 11 тысяч.[1]

Данные были получены из свободного архива Управления уголовного правосудия штата Иллинойс (Illinois Criminal Justice Authority). Первичный источник данных был также общедоступен. Управление делами социального страхования (Social Security Administration) предоставляет подробный индекс записей о смертях (Social Security Death Index, SSDI), включающий имя, дату рождения, номер социального страхования, почтовый индекс последнего места проживания и кое-что еще. Не имея возможности (мы говорим о студентах!) заплатить за получение информации, исследователи использовали *RootsWeb.com* – популярный сайт, посвященный генеалогии – как общедоступный источник данных SSDI. Можно было также воспользоваться общедоступными муниципальными записями актов гражданского состояния.

База SSDI не содержала важных для завершения исследования сведений о поле. Поэтому понадобился еще один источник данных. Студенты нашли недостающее в общедоступной базе данных, распространяемой бюро переписи населения. К тому же, часто можно было определить пол по имени – довольно трудно найти женщину с именем «Роберт» или мужчину, которого бы звали «Сьюзен». После этого оставалось только выполнить компьютерный анализ. Трудно сказать, что́ при размещении баз данных в общем доступе было сделано неправильно, – по отдельности данные почти бесполезны, но вместе взятые они дали больше, чем можно было ожидать.

Чем больше возможностей для реконструкции данных, тем больше *конкретных* решений для противостояния реконструкции приходится изобретать. И тем сильнее опасение, что этот процесс бесконечен. Возможности для реконструкции данных растут с каждой новой базой данных, выложенной в открытый доступ. Все вместе общедоступные базы данных образуют единый фронт цифрового наступления на неприкосновенность частной жизни. В противоположность тому, что мы знаем о соли – ее компоненты натрий и хлор ядовиты, но их химическое соединение в виде соли безвредно, – безобидные базы «очищенных» данных в соединении создают опасную комбинацию. Как с этим бороться?

«Старший Брат» в США и везде

«Старший Брат» ни на секунду не прекращает смотреть на нас, и армия битов только усилила его могущество. В Китае, обладающем большим опытом слежения за гражданами как механизма контроля общества,

[1] Доступ к источникам данных для данного исследования открыт: криминальные сводки по штату Иллинойс – *www.icpsr.umich.edu/NACJD/help/faq6399.html*, индекс записей о смертях – *ssdi.rootsweb.com/*.

миллионы жителей Ченьчжоу получили идентификационные карты, содержимое которых не ограничивалось только именем и адресом получателя. Как следует из отчета «New York Times», карта содержала сведения о стаже работы, образовании, религиозной и этнической принадлежности, наличии судимостей, статусе медицинского страхования, контактах домовладельца и семейном положении.[1] Новая технология (разработанная, кстати, американской компанией) подается под видом мер по борьбе с преступностью и весьма полезна, когда надо выявить участников митинга протеста или просто «подозрительных» граждан. Чем больше страна процветает и чем больше путешествуют ее граждане, тем уместнее с точки зрения власть имущих повальное внедрение подобных технологий – ведь в любой момент можно узнать, где находится тот или иной товарищ. Китайский метод куда эффективнее пресловутых лондонских камер видеонаблюдения.

«Говорите, мы вас слушаем!»

Установка жучков в местах сбора участников криминального или политического подполья всегда была рискованным делом для правоохранительных органов. Есть более безопасная альтернатива, жучок, который многие носят, сами того не подозревая, – мобильный телефон. Многие мобильные телефоны можно удаленно перепрограммировать, так что микрофон всегда включен и аппарат работает на передачу, даже если его владелец считает, что телефон выключен.[2] ФБР использовало этот прием для прослушивания телефонных переговоров Джона Томеро с членами его преступного клана. Федеральный суд постановил, что использование подобного «жучка-маяка» вполне легально.[3] Джон Томеро мог бы предотвратить прослушивание, вынув аккумулятор.[4] Некоторые мнительные бизнесмены так и поступают.

В автомобилях фирмы General Motors, оснащенных системой связи OnStar, микрофон также может быть активизирован из центра связи. Такая функция может спасти жизнь – у оператора компании OnStar есть возможность связаться с водителем, получив сигнал об аварии. Компания честно предупреждает, что «OnStar окажет содействие вы-

---

[1] Кейт Брэдшер (Keith Bradsher) «China Enacting a High-Tech Plan to Track People» (Китай принял план по отслеживанию населения с помощью высоких технологий), *New York Times* от 12 августа 2007 года.

[2] Обратитесь, например, к веб-странице Департамента энергетики, посвященной уязвимостям сотовых телефонов, *www.ntc.doe.gov/cita/CI_Awareness_Guide/V2comint/Cellular.htm*.

[3] Дело «Народ США против Джона Томеро», S2 06 Crim. 0008 (LAK), суд южного округа Нью-Йорка, 462 F. Supp. 2d 565, судья Льюис Каплан, комментарии, 27 ноября 2006 года.

[4] Деклан МакКалло и Энн Броуч (Declan McCullagh and Anne Broache) «FBI taps cell phone mic as eavesdropping tool» (ФБР использует микрофоны сотовых трубок для прослушивания), *CNET News.com*, 1 декабря 2006 года.

полнению судебного постановления, относящегося к уголовному расследованию, инициированному правоохранительными органами или соответствующими службами».[1] ФБР пользуется этой возможностью, чтобы подслушивать беседы в автомобилях. Правда, однажды федеральный суд выступил против подобного способа сбора доказательств – но не в защиту права на неприкосновенность частной жизни. Просто подключение ФБР нарушило нормальный режим работы системы связи OnStar, и суд постановил, что ФБР помешало выполнению договора компании OnStar по обслуживанию клиентов.[2]

Идентификация граждан: нет ID-картам!

В эпоху мирового терроризма демократические страны прибегают к цифровому слежению с целью защиты граждан. Эти меры встречают яростное сопротивление сторонников личной свободы. В США идея национальных идентификационных карт вызывает бурную реакцию даже со стороны тех политических сил, которые обычно не обсуждают личные права и свободы. В соответствии с Актом о присвоении REAL ID (REAL ID act) 2005 года вводится универсальный госстандарт на водительские лицензии. Хотя закон прошел через Конгресс без особых возражений, исполнять его отказались сразу 18 штатов. Точнее, не отказались, а заморозили исполнение сначала до 2009, а затем в начале 2008 до 2011 года. Даже само определение REAL ID в законе далеко от того действительно всеобщего национального ID, который предполагали ввести борцы с преступностью, в частности с терроризмом.

Пока сторонники и противники ID-карт дебатируют, ФБР изобретает новые, более совершенные технологии.

Пока сторонники и противники ID-карт дебатируют, ФБР изобретает новые, более совершенные технологии. Зачем носить с собой технические средства, когда все нужное у человека уже есть? Можно обследовать каждого человека и занести в базу данных его уникальные биометрические данные: отпечатки пальцев; цвет радужной оболочки глаза; тональность голоса; особенности походки; черты лица; следы от повреждений; форму ушной раковины. Можно будет просмотреть съемку группы лиц, свериться с базой данных и получить отчет со списком имен. Удобнее и совершеннее любой карты.

Ну ладно, пока технологии еще не совсем совершенны, но они не стоят на месте. Данные уже накапливаются и заносятся в хранилище Информационной службы уголовного правосудия ФБР (Criminal Justice

---

[1] Страница полезной информации компании OnStar: *www.onstar.com/us_english/jsp/explore/onstar_basics/helpful_info.jsp?info-view=serv_plan*.

[2] Деклан МакКалло (Declan McCullagh) «Court to FBI: No spying on in-car computers» (Суд над ФБР: нет слежению с помощью бортовых компьютеров), *CNET News.com*, 19 ноября 2003 года.

Information Services) в Кларксбурге, штат Западная Виргиния. База данных уже содержит 55 миллионов наборов отпечатков пальцев, и ФБР обрабатывает 100 тысяч идентификационных запросов ежедневно. Любой из 900 тысяч служителей правосудия может отправить запрос и, в случае совпадения, получить досье на подозреваемого.

Трудность состоит в получении отпечатков пальцев; большая часть коллекции ФБР получена при задержании подозреваемых. Поэтому идет поиск решения, как снять возможно больше отпечатков, не привлекая внимания обывателей. К примеру, если в аэропорте повесить объявление вроде «Каждый посетитель подвергается электронному сканированию при пересечении границы зоны досмотра», человек насторожится («это еще зачем?») и, возможно, откажется от полета. Другое дело, когда человек сам говорит себе: «Отпечаток пальца – это уникальный ключ, который всегда со мной и которым я могу открыть проход сюда».[1] При этом, утверждает теория, сбор данных будет добровольным и не вызовет особых возражений.

Плодотворное сотрудничество «Старших Родственников»

Фактически, есть два «Старших Брата», которые часто работают совместно. И мы обычно не возражаем против их заботливого присмотра, если (как нам кажется) знаем, в чем он заключается. Очень редко совместная работа «Старших Братьев» вызывает недовольство.

Первый «Старший Брат» – такой же, как у Оруэлла. Это правительство. Второй – это бизнес. Многие так и не догадываются, что компании ежедневно и непрерывно собирают, объединяют, анализируют и сводят информацию о миллиардах электронных транзакций. Конечно, эти действия компаний не являются шпионажем и не нарушают букву закона, но собранные бизнесом данные о нас чрезвычайно ценны и представляют интерес для обоих «Братьев».

Новая угроза неприкосновенности частной жизни состоит в том, что компьютеры могут выделять ценную информацию из миллиардов ничем не выделяющихся фрагментов данных, аналогично тому как в горнодобывающей промышленности отделяют драгоценные металлы от пустой породы. Компьютеры могут сопоставлять массивы информации, объединяя правительственные и корпоративные базы данных, создавая тем самым подробные досье на миллионы людей. Компьютеры «Старших Братьев», обладая высокими вычислительными мощностями и объемными носителями, могут быстро связывать фрагменты данных не только путем тонкого анализа, как это делали студенты

[1] Эллен Накасима (Ellen Nakashima) «FBI Prepares Vast Database Of Biometrics; $1 Billion Project to Include Images of Irises and Faces» (ФБР создает масштабную биометрическую базу данных; 1 миллиард долларов на коллекцию изображений радужки и лиц), *Washington Post* от 22 декабря 2007 года.

с данными о жертвах убийств, но и простым перебором миллиардов записей. Компьютеры способны отследить даже весьма слабые связи, которые могут оказаться очень важными, например, найти счета террористических организаций или узнать, не замечена ли ваша новая няня в сексуальных домогательствах, или просто рассчитать ставки страхования.

Вернемся к рассказу о правительстве и сборщиках клиентских данных.

Крупнейший сборщик – компания Acxiom. Бизнес Acxiom состоит в накоплении журналов транзакций со всех кредитных карт – в 2004 году регистрировалось более миллиарда транзакций в день. Компания использует свои базы данных для того, чтобы предоставлять банкам, страхователям, компаниям, выдающим кредитные карты, и другим клиентам сведения о том, как люди тратят свои деньги. Само собой разумеется, что после развертывания правительственной компании по борьбе с терроризмом интерес к этим данным и способам их получения проявил и Пентагон. Выявление каналов финансовой помощи террористам могло бы способствовать предотвращению нападений.

Другой крупный сборщик данных в США – компания ChoicePoint. Компания обслуживает более 100 тысяч клиентов, которым требуется проверить некоторого соискателя или кандидата, к примеру для определения страховых рисков.

От других сервисов Acxiom и ChoicePoint отличаются масштабом данных, которыми эти сборщики оперируют. Как было показано в главе 1, количественный рост дает новые качественные эффекты, и это следствие не эволюции технологий, но роста объемов информации. Тридцать лет назад кредитные карты не имели магнитных полос, регистрация оплаты кредиткой производилась механически. Рельефные цифры на ее поверхности отпечатывались через копирку, владельцу кредитки вручался чек, а в компанию, выдавшую карту, отправлялась копия. Сегодня копия суммы наверняка отправится не только в банк, выдавший карту, но и в базу Acxiom или другого сборщика данных, конечно, не на бумаге, а в виде массива битов. Возможность поиска в сверхбольшой корпоративной базе данных информации не только о финансовых транзакциях, но и о телефонных звонках или заказе билетов – еще один пример качественного скачка, происходящего при накоплении чего-либо.

Да, конечно, закон о неприкосновенности частной жизни никто не отменял. Для банка или сборщика данных помещение своей базы данных в открытый доступ будет противоправным действием. Просто законодательство в области защиты личных прав все еще находится в стадии развития, и результат его столкновения с корпоративными или правительственными интересами часто непредсказуем.

Сильный толчок к развитию законодательство о неприкосновенности частной жизни получило во время президентского правления Ричарда

Никсона. Поступок президента Никсона, расцениваемый большинством как вопиющее злоупотребление президентскими полномочиями, заключался в попытке сбора информации о политических оппонентах.[1] По словам нынешнего советника президента, это было «использование государственной машины ради того, чтобы потуже затянуть гайки политическим противникам». Президент Никсон использовал Службу внутренних доходов (Internal Revenue Service), чтобы проверить случаи возврата налогов лицам из «списка врагов», среди которых были конгрессмены, журналисты и наиболее видные жертвователи демократов. Использование Службы внутренних доходов в подобных целях хотя и не было незаконным, было воспринято крайне негативно, поэтому Конгресс запретил возможные попытки такого использования в будущем.

Акт о праве на неприкосновенность частной жизни (Privacy Act) 1947 года четко установил, когда и каким образом правительство США вправе формировать на граждан досье с информацией, не относящейся к расследованию преступлений. Правительство обязано открыто объявить характер и цель сбора информации и в дальнейшем придерживаться этой цели. Акт ограничивает действия правительства в отношении методов сбора и дальнейшего распространения сведений. В частности, «ни одно агентство не вправе никаким образом передавать никакие части хранимых сведений другим лицам исключая передачу упомянутых сведений по предварительному письменному запросу или с предварительного письменного согласия лица, информация о котором содержится в упомянутых сведениях, если не...».[2] Если правительственное агентство допустит неправомерную передачу информации, в том числе другому правительственному агентству, гражданин может обратиться в суд и потребовать компенсации.

Положения Акта предоставляют мощную защиту – впрочем, не столь мощную, как кажется на первый взгляд. Не каждое государственное учреждение является «агентством»; например, это суды. Акт требует публичного оглашения целей и причин сбора сведений, но статья с объяснениями легко может затеряться на страницах «Федерального реестра», куда мало кто заглядывает. Поэтому, скорее всего, эта статья появится в других источниках новостей, но с опозданием. Далее, в тексте Акта есть условие «если не», добавляющее много исключений. К примеру, действие Акта не применяется к распространению информации для статистических, архивных или исторических целей, гражданского или уголовного судопроизводства, расследований Конгресса или запросов, не противоречащих Акту о свободе распространения информации.

---

[1] «Creating a new Who's Who» (Новая версия справочника «Кто есть кто?»), *Time Magazine* от 9 июля 1973 года.

[2] Кодекс законов США, том 5, раздел 552(b).

Несмотря на все допущения, Акт существенно изменил методы работы правительства. Но прошла четверть века, и наступило 11 сентября 2001 года. *Имея возможность соединить все нити, находящиеся в руках разных агентств и ведомств, спецслужбы могли бы предотвратить ужасные события.* Однако Акт о праве на неприкосновенность частной жизни лишил их такой возможности. Потребовались срочные перемены. Первым шагом на пути к построению новой структуры взаимодействия правительственных структур стало создание Департамента национальной безопасности (Department of Homeland Security).

В январе 2002 года, спустя несколько месяцев после нападения на Всемирный торговый центр, Агентство по перспективным оборонным научно-исследовательским разработкам Департамента обороны (Defense Advanced Research Projects Agency, DARPA) создало Отдел информационного снабжения[1] (Information Awareness Office, IAO), цель которого:

> создание идеи, разработка, внедрение, интеграция, демонстрация и модернизация информационных технологий, компонентов и прототипов автоматических информационных систем, способных просчитывать возможность приведения в действие ассиметричных угроз путем анализа необходимой информации; национальное оповещение об угрозе; выдача решений по защите национальной безопасности. Наиболее значимая для США асимметричная угроза – это терроризм, опасность со стороны сети организованных и трудно обнаруживаемых групп людей. Отдел планирует разработать технологию, которая позволит распознавать и выявлять такие сети и группы, узнавать их планы и, возможно, предлагать способы устранения угрозы. Чтобы эффективно и без лишних помех использовать эту технологию для анализа и связывания отдельных фрагментов данных, необходимо обеспечить сотрудничество и обмен данными.

Вице-адмирал Джон Пойндекстер обозначил направление действий, получившее название «Полная информационная осведомленность» («Total Information Awareness», TIA). По его мнению, огромное количество частных хранилищ данных позволяло удобным способом обойти ограничения Акта о праве на неприкосновенность частной жизни. Если Департамент обороны не может получить данные от Службы внутренних доходов, то он *может купить данные у частных сборщиков*! В сообщении электронной почты, датированном маем 2002 года, подполковник Дуг Дайер предложил вице-адмиралу провести переговоры с компанией Acxiom.[2]

---

[1] Описание отдела информационного снабжения можно найти на сайте Информационного центра электронной конфиденциальности: *http://epic.org/privacy/profiling/tia/*.

[2] Сообщение от 21 мая 2002 года; копия выдана 23 января 2004 года Дэвиду Л. Собелу из Информационного центра электронной конфиденциальности по запросу в соответствии с положениями Акта о свободе информации.

Дженнифер Баррет работает в компании Acxiom в качестве юриста и главного специалиста по соблюдению прав граждан на неприкосновенность частной жизни. Она выступила перед Конгрессом и предложила помощь. Одним из ее ключевых предложений было то, что граждане негативно воспримут массовый сбор информации, если перед людьми не будет четкой цели формирования баз данных, понятной всем. Сначала следует выполнять сбор информации, явно необходимой для отслеживания террористических формирований, а затем постепенно привлекать другие данные (хотя невозможно отследить всех террористов, наши нынешние представления о них достаточно близки к истине). Я полностью поддерживаю данный план действий.

В идеале, США нуждаются в информации о коммерческих транзакциях, совершаемых по всему миру. Искомая информация также представляет экономический интерес, поэтому может быть полезна и другим странам. Компания Acxiom располагает всеми возможностями для создания подобной базы данных.

Информация о проекте появилась в *New York Times* в октябре 2002 года.[1] Как заявлял адмирал Пойндекстер, правительство «разрушит преграды», разделяющие агентства, и примет правильное решение о создании цельной картины происходящего из миллиона бессмысленных фрагментов. Публикация вызвала шквал протестов со стороны Информационного центра электронной конфиденциальности и борцов за свободу личности. Конгресс приостановил финансирование плана в 2003 году. Но сама идея не умерла.

Ключевой идеей плана «Полная информационная осведомленность» было просеивание данных, поиск связей и выявление шаблонов, которые могли бы указать на террористическую или иную преступную деятельность. Главное учетное управление в своем отчете по анализу данных (GAO-04-548), находящихся в распоряжении 128 правительственных департаментов, упоминает 199 независимых источников информации, 122 из которых содержат персональные данные.

Хотя выполнение плана «Полная информационная осведомленность» было остановлено, некоторое время существовал похожий на него проект ADVISE, усердно разрабатываемый в Департаменте национальной безопасности. Некоторое время спустя Конгресс постановил, что вследствие замеченных нарушений прав граждан на неприкосновенность частной жизни этот проект также должен быть пересмотрен. В июньском отчете за 2007 год генеральный инспектор Департамента национальной безопасности Ричард Скиннер сообщил, что «руководство проекта не учло необходимость защиты прав граждан перед тем, как начать реализацию трех основных программ», и проект был

[1] Джон Маркофф (John Markoff) «Pentagon plans a computer system that would peek at personal data of Americans» (Пентагон планирует создание компьютерной системы для похищения персональной информации), *New York Times* от 9 ноября 2002 года.

закрыт.[1] Проект ADVISE, однако, был всего лишь одним из 12 параллельно реализуемых проектов систем анализа данных.

По похожим основаниям также был закрыт проект TALON, разрабатываемый в Пентагоне. Целью этого проекта было формирование базы данных отчетов о предполагаемых угрозах для обеспечения защиты объектов как часть более широкой программы национальной контрразведки.[2]

Администрация транспортной безопасности отвечает за досмотр авиапассажиров. Предложенная ей система CAPPS II, в конечном счете отвергнутая по причине нарушения прав граждан, преследовала целью свести воедино различные источники данных, чтобы оценить степень опасности полета, представляемую отдельными пассажирами. Цветные метки показывали, может ли пассажир пройти на борт или остаться для дальнейшего досмотра, либо что его присутствие на борту запрещается.

Правительство создает проекты, СМИ и правозащитные группы указывают на нарушения прав граждан, проекты закрываются и создаются новые. Этот цикл кажется бесконечным. Несмотря на укоренившееся мнение рядовых американцев о том, что правительство пытается установить за ними тотальную слежку, цикл не останавливается, а возобновляется из-за беспокойства тех же граждан о своей безопасности и попыток правительственных структур эту безопасность обеспечить. В конце концов, корпоративные базы данных зачастую содержат гораздо более полную информацию о тех людях, которыми может заинтересоваться правительство.

Смена технологий – смена стиля жизни

Новые технологии создают новые виды общественных отношений. Пока не было дешевых массовых моделей автомобилей, не было и пригородных торговых пассажей. Тридцать лет назад многие избегали самолетов из-за запрета курения; сегодня – из-за запрета пользоваться сотовыми телефонами. Как 2500 лет назад сказал Гераклит, «все течет, все меняется». Некоторые авиалинии уже вводят разрешения на сотовую связь с борта самолета.

Чем больше людей используют новую технологию, тем более полезной она становится. Это можно назвать «цепной реакцией» (см. гла-

---

[1] Майкл Дж. Сниффен (Michael J. Sniffen) «Homeland Security drops data-mining tool» (Спецслужбы отказываются от проекта по сбору и анализу данных), *Washington Post* от 6 сентября 2007 года.

[2] Уолтер Пинкус (Walter Pincus) «Pentagon Will Review Database on U.S. Citizens Protests Among Acts Labeled ‘Suspicious,’» (Пентагон пересмотрит базу данных подозрительных обращений граждан), *Washington Post* от 15 декабря 2005 года.

ву 4). Когда один из авторов получил адрес электронной почты *lewis@harvard*, это было что-то вроде шутки: все, кому можно было отправить сообщение, сидели в одной комнате. Технология электронной почты не могла развиваться, пока ею не начало пользоваться достаточно много людей.

Развитие технологий и общественные перемены взаимосвязаны. Еще одно доказательство этому утверждению – то, что новые традиции, появившиеся с развитием технологий, становятся важнее практических целей, ради которых технологии собственно и разрабатывались. Привыкнув к новому стилю жизни, мы часто не задумываемся, от чего он зависит.

Культура кредитных карт

Полезность сборщиков данных вроде компании Acxiom и ей подобных возрастает пропорционально количеству имен и следов действий с электронными устройствами тех людей, записи о которых поступают в базы сборщиков. Когда кредитные карты были всего лишь разновидностью краткосрочного займа для крупных покупок, данные о кредитках были полезны главным образом для определения вашей кредитоспособности. Теперь, когда с помощью кредиток совершаются покупки на любые суммы, от новых авто до гамбургеров из фаст-фуда, данные о кредитных транзакциях могут помочь воссоздать цельную картину вашей повседневной жизни. Можно узнать, ужинали ли вы сегодня вне дома, как часто вы путешествуете, сколько крепких напитков употребляете. Компании, имеющие дело с кредитными картами, анализируют характер операций, и в этом есть хорошая сторона. Если вы никогда не покидали пределы штата Монтана и вдруг купили алмазный браслет в Рио-де-Жанейро, компьютер кредитной компании выдаст сообщение об отклонении от нормы и кое-кто может поинтересоваться, правда ли, что вы – это вы.

Культура кредитных карт – экономическая проблема для многих американцев, которые используют больше кредитных предложений, чем необходимо, накапливая больше долгов, чем следует. Однако трудно представить массовый отказ от использования кредиток, даже если будет предложена альтернатива на основе RFID-меток. Многие люди обычно носят с собой мало наличности или вовсе не носят, добавляя тем самым все больше информации в базы данных сборщиков.

Культура электронной почты

Электронную почту можно представить как нечто среднее между телефонным разговором и бумажным письмом. Электронная почта передается быстро, как и телефонная связь (сервисы мгновенных сообщений, вроде ICQ, еще быстрее). Сообщение электронной почты может храниться, как бумажное письмо; так же, как бумажное письмо, элект-

ронное сообщение ожидает, пока адресат его прочтет. Но электронная почта в большой степени заменила и то, и другое. Конечно, электронная почта наследует часть недостатков обоих методов связи и добавляет собственные.

Телефонные звонки не могут длиться вечно; их содержание (как правило) не сохраняется, не распространяется среди множества людей, не попадает на стол судье. Отправляя сообщение электронной почты, мы часто забываем, что оно не исчезает после отправки или прочтения. Даже Билл Гейтс желал бы, чтобы сообщения не могли храниться вечно. После выступления на слушании антимонопольного дела, где Билл Гейтс заявлял, что он не собирался заключать сделку по разделению рынка броузеров с конкурентом, суд предъявил внутрикорпоративное сообщение, явно опровергающее это заявление: «Мы могли бы даже заплатить им за сделку, купив часть их активов или предложив что-то в этом роде».[1]

Электронная почта – это поток битов, путешествующий по Интернету через вашего интернет-провайдера с применением программного обеспечения, которое может создавать копии, фильтровать спам или проходить другую обработку. Если ваша почтовая служба – компания Google, то вы увидите рекламу. Если вы работаете в финансовой корпорации, ваши сообщения скорее всего заносятся в базу данных – даже если вы писали своей бабушке – просто ради того, чтобы корпорация могла восстановить ход событий, если что-то случится.

До тех пор пока не применяется шифрование, что встречается редко, электронная почта так же открыта миру, как почтовая открытка.

До тех пор пока не применяется шифрование, что встречается редко, электронная почта так же открыта миру, как почтовая открытка. Работодатели нередко сохраняют за собой право читать сообщения электронной почты компании. Взгляните на правила своей компании; возможно их будет трудно найти; возможно, в них говорится совсем не то, чего вы ожидаете. Вот, к примеру, выдержки из правил Гарвардского университета:

> Сотрудники не могут рассчитывать на неприкосновенность того, что они создают, хранят, отправляют или получают с помощью компьютеров, вычислительных сетей или систем связи Университета... Доступ к текстовым файлам, сообщениям электронной почты, файлам данных, изображений, программ или голосовой почты может быть в любое время получен руководством или другими уполномоченными лицами для

[1] В этом сообщении, отправленном Биллом Гейтсом в 1995 году, акцентирована роль электронной почты. Цитируется Стивом Лором при рассмотрении антимонопольного дела, *New York Times* от 2 ноября 1998 года.

любых организационных целей. Доступ может быть запрошен и предоставлен через другого пользователя системы, хотя и не обязательно.[1]

Работодателям просто необходимо обладать такими широкими полномочиями, чтобы вести собственные расследования (конечно, в рамках закона). В сущности, такая политика не представляет проблем для работников, если те, кто имеет доступ к информации, обладают высокими моральными качествами. В Гарварде, к счастью, с этим нет проблем. Хотя общее правило таково, что большинство из тех, у кого есть право рыться в чужих записях, не устоят перед искушением и сделают это даже без особой причины.

Коммерческие серверы электронной почты могут хранить копии даже удаленных пользователем сообщений. Кроме того, есть немало бесплатных серверов, таких как Google, Gmail, Yahoo! Mail или Microsoft Hotmail. Можно обеспечить безопасность электронной почты с помощью шифрования, к примеру, применяя специальное программное обеспечение или шифрующие серверы электронной почты, например Hushmail – бесплатный сервер веб-почты, обеспечивающий шифрование сообщений по технологии PGP (см. главу 5). Таких сервисов, конечно, меньше, чем их небезопасных аналогов. Почтовый сервис Google бесплатен и вполне надежен, однако часть экрана займет реклама. Удобство и бесплатность заставляют забыть о праве на неприкосновенность частной переписки. Все-таки большинство пользователей бесплатных сервисов не задумываются о том, что вся их почта хранится у компании Google или ее конкурентов, как если бы почтовая служба хранила копии всех бумажных писем. Мы так привыкли к сервису, что уже не замечаем его.

Веб-культура

Отправляя сообщение электронной почты, мы, по крайней мере *отчасти*, пытаемся произвести некоторое впечатление, так как все же общаемся с конкретным человеком. В письме можно написать то, что трудно сказать при личной встрече или о чем придется пожалеть. Поскольку невозможно увидеть ответную человеческую реакцию, в письме мы можем позволить себе быть более ироничными, сердитыми или остроумными. Для отправки электронной почты нужен адрес, и мы предполагаем, что читать наше сообщение будет только тот, кому оно адресовано.

Другое дело Всемирная паутина. Социальные сети произошли не от телефонных звонков или писем – скорее, от досок объявлений. Напечатайте комментарий в блоге или выложите фотографии в фотоальбо-

[1] Инструкции для руководящего/преподавательского состава, а также обслуживающего персонала Гарвардского университета, раздел 2.6.С (декабрь 2007 года).

ме – и ваше действие может остаться настолько анонимным, насколько вы пожелаете, но, скорее всего, вы не узнаете, к кому попали ваши сообщения или файлы.

Сервис YouTube хранит миллионы частных видеороликов. Другие сервисы могут хранить архивы фотографий – фотоальбомы XXI века. Сервисы онлайн-архивации предоставят вам часть места на своих носителях для хранения содержимого ваших дисков. Мы беззаботно доверяем им наши коммерческие тайны и личную информацию. Поколение, выросшее вместе со Всемирной паутиной, раскрыло объятия социальным сетям и блогам всех видов и размеров: MySpace, YouTube, LiveJournal, Facebook, Xanga, Classmates.com, Flickr и др. Это уже не похищение, а добровольная выдача своих личных тайн в слепом следовании примеру других.

Капитуляция индивидуальности – уже больше, чем способ установления контактов, это образ жизни в новом обществе. Около 70 миллионов блоггеров ежедневно пишут обо всем подряд – от незначительных мелочей до самых глубоких личных тайн. Сайты вроде *www.loopt.com* позволяют находить новых друзей, а на сайте *twitter.com* вы можете сообщить всему свету, где вы и что делаете. Всемирная паутина – это запутанная, неорганизованная, хаотичная реальность, полная как ценностей, так и мусора.

Прежняя форма Всемирной паутины, Web 1.0, была всего лишь информационным ресурсом. Вы что-то запрашивали и получали ответ. То непонимание принципов функционирования, которое возникает при работе с социальными сетями нового типа (Web 2.0), вызвано тем, что дизайн подобных сетей все еще вызывает эффект нахождения «по ту сторону экрана», то есть просто просмотра, без цифровых отпечатков, особенно при использовании псевдонимов, или «ников» (более подробно разница между Web 1.0 и Web 2.0 обсуждается в главе 4).

На самом деле, Всемирная паутина работает иначе. Важно понимать, что и форма Web 1.0 не позволяла оставаться полностью анонимным, даже если вы «просто смотрели».

В июле 2006 года сотрудник *New York Times* позвонил Тельме Арнольд, жительнице Лильбурна (штат Джорджия). Женщина не ждала этого звонка. Она не была знаменита, не отличалась чем-то особенным. Тельма Арнольд посвящала время своим увлечениям, помогала друзьям и время от времени искала информацию в Интернете – материалы о собаках или о лечении.

Тельма Арнольд обычно использовала поисковую систему AOL и едва ли догадывалась, что все ее запросы сохраняются. Компания-владелец решила поделиться с научным миром частью истории поисковых запросов. Под влиянием приступа необдуманной щедрости компания AOL все же открыла для свободного использования лишь малую толику – около 20 миллионов запросов от 658 тысяч пользователей. По ны-

нешним меркам, немного.[1] К примеру, известно, что в июле 2007 года пользователи Интернета сделали около 5,6 миллиарда запросов к поисковым системам, примерно 340 миллионов из которых пришлись на долю системы AOL. В попытке защитить частную жизнь пользователей, компания AOL «очистила» данные, заменив имена случайными числами. Тельма Арнольд проходила под номером 4417149. Как мы уже знаем, такой «грубой очистки» совершенно недостаточно.

Установить личность Тельмы Арнольд по ее запросам было несложно. Она указывала в запросах «пейзажисты в Лильбурне, Джорджия», а также несколько раз фамилию Арнольд, чтобы узнать, есть ли в однофамильцы ее городе. Многие запросы не были особенно полезны для идентификации, но позволяли больше узнать о ней: «сухость во рту», «щитовидная железа», «собаки, которые везде мочатся» и «детские игровые комплексы».

Тельма Арнольд была не единственной, кого идентифицировали. Пользователь с номером 22690686 (Терри) любит астрологию и пиво Budweiser, интересуется состоянием банка Edison National Bank и финансовой компании Primerica. Пользователь с номером 5779844 (Лаванна) ищет информацию по кредитным отчетам и школам. А судя по запросам пользователя с номером 356693, он является помощником Криса Шэйса, конгрессмена от штата Коннектикут.

Один из доступных нам способов борьбы с цифровым вторжением в частную жизнь – это обрывочная, лишенная контекста информация. Было ли у Тельмы Арнольд множество болезней? Судя по содержанию ее запросов, да. На самом деле, она хотела помочь своим друзьям.

А вот журнал запросов пользователя номер 17556639:

как убить свою жену 23.03, 22:09
убийца жены 23.03, 22:11
истощение 23.03, 22:12
мертвые люди 23.03, 22:13
снимки мертвых людей 23.03, 22:15
убитые люди 23.03, 22:16
мертвецы фотографии 23.03, 22:17
фотография убийство 23.03, 22:20
фотография смерти 23.03, 22:30
смерть 23.03, 22:33
мертвые люди фотографии 23.03, 22:33
фотографии мертвых людей 23.03, 22:35
www.murderdpeople.com 23.03, 22:37

[1] Денни Салливан (Danny Sullivan) «Nielsen NetRatings Search Engine Ratings» (Оценка поисковых систем Nielsen NetRatings), *Search Engine Watch* от 22 августа 2006 года.

обезглавленные люди фотографии 23.03, 22:39
автомобильные аварии 23.03, 22:40
автомобильные аварии фото 23.03, 22:41

Не преступник ли этот пользователь? Должна ли компания AOL обратиться в полицию? Планирует ли номер 17556639 убийство своей жены? Или он исследователь, писатель? В данном случае обращение в полицию – это гражданский долг или вторжение в частную жизнь?

Невозможно установить только по этим запросам, планирует ли пользователь какое-то жуткое действо или наводит справки для нового романа, содержащего несколько душераздирающих эпизодов. Когда информация неполна или оторвана от контекста, трудно распознать намерение или цель.

В данном конкретном случае мы знаем ответ. Пользователь по имени Джейсон из штата Нью-Джерси просто дурачился, пытаясь выяснить, наблюдает ли за ним «Старший Брат». Он вовсе не собирался убивать свою жену.[1] Делая выводы из неполных данных, не следует забывать, что из неполных или ложных посылок вероятнее всего следует ложное заключение, особенно если мыслить стереотипно.

Интерпретировать данные следует осторожно, чтобы, с одной стороны, защитить общество от возможной угрозы, а с другой, не допустить ошибочных обвинений. В каждом случае сомнительной интерпретации данных может помочь только накопление большего их количества без вторжения в частную жизнь.

За границами частной жизни

Ничто не ново под луной, и все усилия по определению понятия и соблюдению права граждан на неприкосновенность частной жизни не исключение. История показывает, что наше понимание данного права развивается, а вместе с ним развивается и законодательство. После вторжения цифровых технологий в нашу жизнь мы оказались в точке, с которой развитие начало ускоряться.

Оставьте меня в покое

Больше века назад два юриста подняли тревогу, обеспокоенные воздействием, которое технологии и СМИ оказывают на неприкосновенность частной жизни:

> Мгновенные снимки и газетная индустрия вторглись в святая святых – частную и личную жизнь; множество механических устройств угрожало воплотить в жизнь предсказание о том, что «шепот в подвале может гулко отозваться на чердаке».

[1] *thesarc.blogspot.com/2006/08/aol-user-says-just-kidding-about.html.*

Это выражение взято из одной из первых обзорных правовых статей по праву на неприкосновенность частной жизни, которую в 1890 году опубликовали бостонский адвокат Сэмюэл Уоррен и его партнер Луис Брэндис[1], позднее ставший членом Верховного суда. Уоррен и Брэндис продолжают: «Сплетни и слухи больше не являются уделом праздных и порочных людей; теперь они стали предметом торговли, за которым гонятся как индустрия, так и бесстыдство. Чтобы удовлетворить праздное любопытство, в дневных колонках часто появляются самые откровенные и интимные подробности. Чтобы занять досуг, колонка за колонкой заполняются пустыми сплетнями, которые могут быть получены только путем вторжения в семейный круг». Новые технологии позволяют легко производить подобный мусор, а там уже «предложение рождает спрос».

И эти откровенные фотографии и колонки, заполненные сплетнями, были не просто безвкусными; они были просто плохими. Почти в тех же выражениях, какие нынче употребляют критики бездушных телевизионных реалити-шоу, Уоррен и Брэндис увлеченно доказывают, что общество катится в тартарары из-за всего этого мусора, распространяемого вокруг.

> Безобидные сплетни обретают недобрую силу, когда распространяются и закрепляются в умах людей. Сплетни принижают и извращают понимание действительности. Они ставят с ног на голову степень важности вещей, мешая росту мысли и духовному развитию людей. Когда мелкий слушок обретает долговечность печатного слова, вытесняя из умов то, что действительно важно, не удивительно, что зеваки и невежды принимают желаемое за действительное. Сострадание к беде соседа никогда не бывает полностью искренним, людей привлекает возможность послушать о несчастьях других. Банальность разрушает в одночасье и строгость мышления, и возвышенность чувств. Ее приземляющее влияние заглушит любой подъем чувств, любой благородный порыв.

Суть проблемы, обозначенной Уорреном и Брэндисом, состояла в том, что трудно было признать факт вторжения в личную жизнь правонарушением. В отдельных случаях возможно было назначить наказание, но общепринятой судебной практики не существовало. Судьи нередко приговаривали к наказанию за умышленное распускание ложных слухов. Однако нельзя было наказывать за умышленное распространение истинных сведений. Другие суды могли назначить наказание за опубликование частных писем, но делали это исходя из понятий права собственности – другими словами, письма являлись имуществом и были украдены, как, например, конокрад украл лошадь. Уоррен и Брэндис считают такой подход ошибочным и далеким от сути дела. По их мнению, когда какая-то информация приватного характера о вас становится достоянием общественности, вы вправе считать себя жер-

[1] Сэмюэл Уоррен и Луис Брэндис (Samuel Warren and Louis Brandeis) «The Right to Privacy» (Право на неприкосновенность частной жизни), *Harvard Law Review*, IV, 5 (15 декабря 1890 года).

твой воровства: у вас украли часть вашей личности. Уоррен и Брэндис считают, что «фундаментальное право каждого остаться наедине с самим собой» является естественным правом человека. Это право долго оставалось «за кадром» судебных разбирательств, но новые технологии вывели его «на передний план». В статье правозащитников также упоминается, что в определении нового права они опирались на принцип «неприкосновенности личности».

Неприкосновенность частной жизни и свобода

Определение права каждого на личную жизнь, данное Уорреном и Брэндисом, было важным, но не полным. В XX веке было слишком много причин *не* оставлять людей в одиночестве и слишком много способов их *объединения*. В США Первая поправка к Конституции, разрешив свободу слова, встала на пути к свободе одиночества. Как правило, правительство просто не может запретить каждому высказать *любое* свое мнение. В частности, правительство не может запретить мне говорить все, что мне вздумается, о ваших личных делах. Определение Уоррена–Брэндиса все же работало, и достаточно долго, так как, по словам профессора информатики Роберта Фано, «темп технического прогресса долгое время был достаточно медленным для того, чтобы общество училось противостоять злоупотреблениям технологическими достижениями и большую часть времени сохранять равновесие сил».[1] Но с конца 1950-х появление электроники, компьютеров и вычислительных сетей нарушило равновесие. Общество перестало успевать реагировать на развитие очередных технологий слежения.

Ассоциация юристов Нью-Йорка (Association of the Bar of the City of New York) провела глубокое исследование, вершиной которого стала публикация в 1967 году книги профессора Колумбийского университета Алана Уэстина (Alan Westin) «Неприкосновенность частной жизни и свобода» («Privacy and Freedom»). (Приведенные выше слова профессора Фано – результат знакомства с данной книгой.) Профессор Уэстин предложил резкую смену точки зрения.

Уоррен и Брэндис рассматривали вторжение в личную жизнь как разновидность нанесения персонального ущерба, который мог «вызвать душевную боль и расстройство значительно большие, чем простое физическое ранение». Согласно мнению профессора Уэстина люди должны брать ответственность на себя, защищаясь самостоятельно. «Каждый человек должен нести ответственность только за свои действия и проступки». Но закон обязан обеспечить людей оружием, с которым можно противостоять вторжениям в частную жизнь.

---

[1] Р. М. Фано (R. M. Fano) «Review of Alan Westin's Privacy and Freedom» (Обзор книги Алана Уэстина «Неприкосновенность частной жизни и свобода»), *Scientific American*, май 1968 года, с. 148–152.

Профессор Уэстин поясняет, что формулировка Уоррена–Брэндиса слишком идеальна и не учитывает права людей на свободу слова и правомерные общественные практики сбора статистики. В качестве мер защиты следует избрать не «глухую оборону» и «стену молчания», а контроль способов использования персональной информации. «Неприкосновенность частной информации, – пишет профессор Уэстин, – это законное право отдельных лиц, групп или организаций на самостоятельное определение того, когда, как и в каком объеме делиться информацией о себе с другими».

> ...необходим четко определенный и обоснованный процесс оценки с определением критериев того, какие средства общественных и частных властных структур для разоблачения и слежения могут быть применены в сравнении со степенью правомерности использования таковых средств и мерой вторжения в частную жизнь. Предлагается базовый план такового процесса: оценка степени необходимости установления наблюдения; принятие решения о целесообразности использования альтернативных средств; оценка степени достоверности получаемой информации; определение правомерности принятия решения об установлении наблюдения; оценка правоспособности ограничения и контроля наблюдения, если это возможно.

Следовательно, даже если правительство или кто-то другой вправе осуществлять сбор информации о вас, в вашем праве ограничить диапазон возможного применения полученной информации.

Такое более тонкое понимание права на неприкосновенность частной жизни произошло из понимания того значения, которое личная информация имеет в обществе. Это право заключается не в возможности изоляции от общества (по Уоррену и Брэндису), а в регулировании функционирования самого общества. Профессор Фано выделил три социальных роли права на неприкосновенность частной жизни. Во-первых, «право сохранять личную информацию в тайне может пониматься как часть права на жизнь и самосохранение», – храните свои подростковые переживания и внутренние конфликты при себе, если они не мешают вам занимать свое место в социуме. Во-вторых, с помощью права каждого на неприкосновенность частной жизни осуществляется возможность отклонения от нормы общественного поведения в том смысле, что ни один набор общественных норм и правил потенциально не является совершенным и идеально подходящим для всех, а также в том смысле, что социальный прогресс требует социального экспериментирования. В-третьих, наличие права держать свои тайны при себе способствует развитию независимости мышления, для чего требуется известная степень уединенности и, возможно,

Право на неприкосновенность частной жизни допускает отклонения от преобладающих в обществе норм, помогая этим социальному прогрессу, для которого требуется социальное экспериментирование.

обсуждение своих мыслей в более узком кругу, прежде чем представить их на суд общества.

«Неприкосновенность частной жизни и свобода», а также политика правительственных агентств и корпораций в 1960-х побудили умы к переоценке значения прикладного применения прав на частную жизнь. О чем на самом деле думают хозяева огромного банка данных, когда накапливают, обрабатывают и передают данные другим?

Принципы добросовестного использования информации

В 1973 году Департамент здравоохранения, образования и социальной поддержки (Department of Health, Education, and Welfare) опубликовал следующие «Принципы добросовестного использования информации» («Fair Information Practice Principles», FIPP):

- **Открытость.** Не должно быть систем хранения персональных данных, существование которых скрыто от общества.
- **Доступность.** У каждого лица, запись о котором есть в системе хранения персональных данных, должна быть возможность узнать содержание этой записи и то, как оно используется.
- **Повторное использование.** У каждого лица, запись о котором есть в системе хранения персональных данных, должна быть возможность запретить использование записи в целях, отличных от предполагаемой, без его согласия.
- **Исправление.** У каждого лица, запись о котором есть в системе хранения персональных данных, должна быть возможность исправлять данные, способствующие его возможной идентификации.
- **Безопасность.** Любая организация, создающая, поддерживающая, использующая или распространяющая записи, содержащие персональные или способствующие идентификации данные, должна обеспечить использование данных только по прямому назначению и принять меры к недопущению ненадлежащего использования данных.[1]

Первоначально эти принципы предназначались для защиты медицинских данных, однако никогда не были законодательно закреплены. Но все же они стали основой для многих корпоративных политик безопасности частных данных. Частично принципы добросовестного использования информации вошли в международные торговые соглашения в рамках Организации экономического сотрудничества и развития в 1980 году и Европейского Союза в 1995 году. В США эти принципы

[1] Консультативный совет по автоматизированным системам обработки персональных данных и соблюдению прав граждан. Текст предоставлен Информационным центром электронной конфиденциальности, *www.epic.org/privacy/consumer/code_fair_info.html*.

прослеживаются в законодательстве некоторых штатов, но федеральные законы обращаются к принципам от случая к случаю или только в определенных областях права («секторный подход»).[1] Акт о праве на неприкосновенность частной жизни регулирует передачу данных между правительственными агентствами, но никак не ограничивает частный оборот данных. Акт о добросовестной отчетности по кредитованию (Fair Credit Reporting Act) применяется только к данным потребительского кредитования и игнорирует медицинские записи. Акт о защите персональной информации при использовании видеопродукции описывает обращение с прокатом видеокассет и ничего не говорит о скачивании видеофайлов, которых на момент принятия акта попросту не было. Наконец, лишь малое число федеральных или местных правовых актов применимо к большим банкам данных городских архивов. Американское правительство по сути децентрализовано, и управление правительственными данными также децентрализовано.

США не испытывают недостатка в законах о праве на неприкосновенность частной жизни. Однако существующее законодательство недостаточно четко и порой противоречиво; кроме того, оно слишком привязано к технической терминологии. Нет общенационального соглашения о предмете и методах защиты. Без более детальной проработки, согласования деталей и информирования судейского состава текущая правовая путаница может со временем только ухудшаться.

Законодательство США о праве на неприкосновенность частной жизни

Совет комитетов по совершенствованию бизнеса (Council of Better Business Bureaus) выпустил «Обзор федеральных и местных законов о праве на неприкосновенность частной жизни» (*www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf*).

Правительство штата Техас также выпустило краткую сводку основных законов о праве на неприкосновенность личной жизни (*www.oag.state.tx.us/notice/privacy_table.htm*).

Расхождение правовых стандартов США и Европы стоит на пути развития международной торговли, так как директивы Евросоюза запрещают передачу конфиденциальных данных странам, которые не отвечают европейским стандартам «адекватности» защиты приватной информации. Хотя американский «секторный подход» все еще далек от требований ЕС, в 2000 году Еврокомиссия создала «тихую гавань» для сделок американских бизнесменов с европейскими. Это позволило отдельным

[1] *www.export.gov/safeharbor/*

корпорациям привести свои методы работы в соответствие с семью принципами: оповещение, выбор, непосредственная передача, доступ, безопасность, целостность данных и последовательное воплощение.

Можно долго спорить о том, что всеобъемлющий европейский подход более фундаментален, чем основанный на прецедентах американский, в то время как главный вопрос состоит в том, какой подход на самом деле отвечает нашим нуждам. Акт о праве на неприкосновенность частной жизни гарантирует нам, что официальное объявление правительства о начале очередной кампании по сбору информации будет надежно укрыто в чаще страниц «Федерального реестра», – лучше, чем полное молчание, однако «открытость» при таком подходе присутствует только формально. Большинство крупных корпораций, обслуживающих массового потребителя, предъявляют документы о политике безопасности личной информации, но эти документы почти никто не читает. К примеру, в 2002 году лицензионные соглашения читали только 0,3% пользователей сервиса Yahoo!. В том же году под давлением массы негативных откликов, которые появились после рассылки рекламы, компания включила в лицензионные соглашения пункт о разрешении публикации рекламы; количество пользователей сервиса Yahoo!, прочитавших тексты соглашений выросло всего лишь до 1%.[1] Все имеющееся законодательство США не смогло предотвратить ни программу прослушивания телефонных разговоров граждан, введенную администрацией Буша, ни вовлечение в программу крупнейших телефонных операторов страны.

На самом деле из-за дальнейшего развития технологий сотрудничество правительства и отдельной отрасли кажется более важным, чем когда бы то ни было, для сбора информации о наркотрафике и международном терроризме. 20 лет назад большинство междугородных и международных звонков какую-то часть пути преодолевали по радиоволнам с помощью антенн, работающих в ультракоротковолновом диапазоне, или через спутник связи. Спецслужбы могли просто и быстро подключиться к ним (см. обсуждение системы ECHELON в главе 5). В настоящее время многие звонки передаются по оптоволоконным кабелям, поэтому правительство настойчиво ищет возможности подключения к этой частной инфраструктуре.[2]

Хорошая безопасность стоит дорого. Высокие расходы могут ограничить ценность данных для общества. Опасения общественности насчет возможных утечек медицинской информации привели к значительным пополнениям в законодательстве. Акт об учете и передаче медицинских

---

[1] Сол Ханселл (Saul Hansell) «Compressed data: The big Yahoo privacy storm that wasn't» (Сжатые данные: мощный Yahoo-шторм личных данных, которого не было), *New York Times* от 13 мая 2002 года.

[2] Эрик Лихтблау, Джеймс Райзен, Скотт Шейн (Eric Lichtblau, James Risen, Scott Shane) «Wider spying fuels aid plan for Telecom industry» (Расширение возможностей шпионажа питает план помощи для индустрии телекоммуникаций), *New York Times* от 16 декабря, 2007 года.

данных (Health Information Portability and Accountability Act, HIPAA) направлен одновременно на поощрение безопасного обмена медицинскими данными и на строгое наказание за утечку «защищенной медицинской информации» – обширной категории, под которую подпадают истории болезней, сведения об оплате медицинских услуг и другие данные. Акт устанавливает необходимость удаления из медицинских записей всех данных, которые могли бы указать на их источник. Применение акта чревато проблемами в мире вездесущих цифровых данных и мощных компьютеров. Вычислительная мощь и способность компьютеров объединять фрагменты, выявляя их связь, делают почти невозможным достижение требуемой законом степени анонимности. Помощь приходит неожиданно и за соответствующую цену со стороны новой отрасли HIPAA-консультантов. Обратившись к поисковой системе с соответствующим запросом, вы, скорее всего, увидите рекламные объявления сервисов, которые помогут вам не только защитить свои данные, но и избежать излишнего внимания со стороны правоохранительных органов.

Читаете ли вы лицензионные соглашения?

До тех пор пока вы соглашаетесь с ними не глядя, компании могут делать с вашей личной информацией все, что угодно. С этим трудно спорить, но многие потребители сами на это напрашиваются, принимая условия лицензионных соглашений. Корпорация Sears Holding, родительская компания сетей розничной торговли Sears, Roebuck и Kmart, предлагает клиентам вступить в сообщество «Мой круг Sears Holding», которое компания описывает как «динамичное и интерактивное онлайн-сообщество... где ваш голос всегда слышен и ваше мнение всегда имеет вес». При регистрации на экране появляется окно. Видимая область с полосой прокрутки вмещает только 10 строк текста, а все соглашение занимает 54 «страницы». Набравшись терпения, можно найти в тексте такие условия, как: вы разрешаете компании устанавливать на ваш компьютер программное обеспечение, которое «осуществляет мониторинг всей интернет-активности... включая заполнение «корзины», заполнение формы или проверку вашей... личной финансовой или медицинской информации». Итак, ваш компьютер может отправить корпорации Sears Holding вашу кредитную историю или результаты теста на ВИЧ, а вы с этим радостно согласились![1]

[1] Бен Эдельман (Ben Edelman) «The Sears ‘Community’ Installation of ComScore» (Установка программного обеспечения Sears), *www.benedelman.org/news/010108-1.html*.

Законы о неприкосновенности частной жизни, защищая нашу персональную информацию, в то же время делают затратными или даже невозможными медицинские исследования. Классические исследования, вроде тех, что проводила Фрамингемская группа исследователей болезней кровообращения, исследовавшая тысячи добровольцев, не могут быть повторены в современной среде с развитой политикой анонимности. Доктор Роберта Несс, президент Американского эпидемиологического колледжа, заявляет: «Похоже, применение положений Акта об учете и передаче медицинских данных может даже негативно сказаться на общепринятых практиках обследования здоровья населения».[1]

Европейский подход к анонимности, основанный на «Принципах добросовестного использования информации», зачастую не лучше американского. Пройдитесь по Лондону и поищите таблички с надписью «Warning: CCTV in use» («Осторожно, работают камеры наблюдения»). Вот вам и принцип «открытости»! Подобные таблички встречаются по всему городу, и они едва ли служат признаком доверия гражданам. Даже «Старший Брат» из романа Оруэлла соблюдал этот принцип: «СТАРШИЙ БРАТ СМОТРИТ НА ТЕБЯ».

Принцип «повторного использования» регулярно нарушается в некоторых европейских странах, при том что удовлетворение принципам анонимности – основная административная нагрузка на европейских бизнесменов, и пренебрежение принципами может, как минимум, приостановить бизнес, заставляя как следует подумать, прежде чем «сменить ориентиры» использования данных.

Социолог Амитаи Этциони проведя много опросов европейской аудитории на предмет того, спрашивали ли разрешения граждан на повторное использование их персональной информации, получил только один положительный ответ об одной американской компании.[2]

«Принципы добросовестного использования информации» и их тень в виде незащищенности и персонального контроля несомненно улучшили методы соблюдения неприкосновенности частной жизни. Но их сокрушил цифровой взрыв вкупе с враждебностью этого мира, а также социальными и культурными изменениями повседневности. Фред Кейт, исследователь приватности из Университета Индианы, характеризует «Принципы...» как полный провал:

---

[1] По мнению ученых, «законы о неприкосновенности частной жизни тормозят и делают более затратными научные исследования», *Science Daily* от 14 ноября 2007 года, *www.sciencedaily.com/releases/2007/11/071113165648.htm*.

[2] Данные приводит Фред Кейт (Fred Cate) в главе «The failure of Fair Information Practice Principles» (Падение принципов добросовестного использования информации) книги Джейн К. Уинн (Jane K. Winn) «Consumer Protection in the Age of the „Information Economy“» (Защита потребителя в эпоху «информационной экономики»), Ashgate, 2006.

Современное законодательство, защищающее право на неприкосновенность частной жизни, зачастую обременительно, затратно, бюрократично и предлагает удивительно низкий уровень защиты. Установленная возможность индивидуального контроля воплощается на практике крайне редко. В мире, который из-за информационных технологий, международной торговли и быстрых средств передвижения быстро идет к глобализации, законодательство о защите данных выросло искривленным и слабо приспособленным. Это законодательство отошло от своих первоначальных принципов, которые сами по себе представляли нестройную смесь. Повторение „Принципов…“ как заклинания больше не поможет скрывать тот факт, что „король-то голый“ и что необходимо „сшить новое платье“».[1]

Право на неприкосновенность частной жизни как право контролировать информацию

Настало время признать, что мы сами толком не знаем, чего хотим. Биты обитают повсюду: от них нельзя отгородиться, да почти никто к этому и не стремится. Значение понятия права на частную жизнь изменилось, и мы не знаем, как его определить. Это явно не право остаться в одиночестве, потому что даже самые экстремальные обстоятельства не смогут отдалить нас от влияния цифровых технологий. Это и не право хранить нашу личную информацию в строгой тайне, потому что многие миллиарды мелких фактиков не могут быть однозначно оценены как частные или публичные.

Биты обитают повсюду: от них нельзя отгородиться, да почти никто к этому и не стремится.

Рид Селигманн, возможно, ценил свое право на частную жизнь больше, чем любой другой современный американец. 17 апреля 2006 года Селигманну было предъявлено обвинение в соучастии в изнасиловании 27-летней танцовщицы на закрытой вечеринке. Ему и другим членам команды по лакроссу Университета Дьюка, также обвиненным в соучастии, пришлось бы туго если бы присяжные, располагая только одной положительной характеристикой, дожидались их разрешения на просмотр накопленных персональных данных. Он и его предполагаемые соучастники сразу ощутили на себе такой шквал национальной ненависти за подрыв всех возможных устоев американского общества, что его не сдержали бы даже Уоррен и Брэндис, появись они вдруг. Рид Селигманн отрицал обвинения, и довольно долго слушание шло в духе взаимных голословных утверждений, заверений и обращений к поведенческим стереотипам.

[1] Фред Кейт (Fred Cate) «The failure of Fair Information Practice Principles» (Падение принципов добросовестного использования информации).

Однако во время той закрытой вечеринки Селигманн оставил цифровой след. Этот след свидетельствовал о том, что обвиняемый не мог пробыть на вечеринке достаточно долго и во время предполагаемого совершения преступления занимался другими делами. Фотографии участников веселья имели временные метки, из которых следовало, что в 12:02 предполагаемая жертва свободно танцевала. В 12:24 Селигманн воспользовался своей кредиткой **ATM в банке, о чем имелась** соответствующая банковская запись. В 12:25 обвиняемый звонил по сотовому телефону; информация об этом была предоставлена сотовым оператором. В 12:46 обвиняемый предъявил свой пропуск при входе в общежитие, что зафиксировал университетский компьютер. Примерно так же перемещения **RFID**-меток регистрируются там, где есть ридеры. Рид Селигман всего лишь перемещался по территории университета, но почти каждый его шаг мог быть вычислен. Если бы обвиняемый перемещался на дальние расстояния или жил вне кампуса, то его защитник не имел бы возможности воспользоваться решающими доказательствами.[1]

Итак, что вы предпочтете: новый мир, в котором каждый шаг оставляет цифровой след и неотъемлемый атрибут которого – постоянное ощущение слежки, или старый мир, где цифровых следов почти нет и где меньше подглядывающих глаз? И какой смысл в предыдущем вопросе, если мир нельзя вернуть в прежнее состояние?

В мире, где неприкосновенность частной жизни уже не является стеной, окружающей индивидуума, следует контролировать список тех, к кому может *попасть* ваша персональная информация. Разместив на YouTube ролик, где танцую голым, я, скорее всего, столкнусь с некоторыми неприятными последствиями этого поступка. В конце концов, по словам Уоррена и Брэндиса, каждый должен отвечать за свои действия. Однако общество установило границы приватности и связи между поступками и последствиями. Возможно, для компенсации размытия границ понятия частной жизни следует уточнить границы ответственности. Как объясняет Дэниел Вайтцнер, преподаватель и исследователь проблем электронной анонимности:

> Новое поколение законов о праве на неприкосновенность частной жизни должно усилить ограничение использования персональной информации для защиты от дискриминации на основе даже общедоступных данных. К примеру, потенциальный работодатель может увидеть, как соискатель работы входит в мечеть или в диспансер. Хотя гражданин мог уже опубликовать данную информацию, новые законы должны

[1] Крис Куомо, Эрик Аврам, Лара Сетракян (Chris Cuomo, Eric Avram, and Lara Setrakian) «Key Evidence Supports Alibi in Potential Rape Defense for One Indicted Duke Player» (Решающие доказательства спасают игрока Университета Дьюка от обвинения в изнасиловании), *ABC News*, *abcnews.go.com/GMA/LegalCenter/story?id=1858806&page=1.*

> удержать работодателя от решения об отказе на данном основании и назначить строгое наказание в случае такого отказа.[1]

Продолжая в том же духе, публикация списков избирателей и политических пожертвователей не является ошибкой. Такая публикация – важный элемент нормального функционирования американской демократии. Отказ кому-либо в содействии из-за его политических предпочтений *был бы* ошибкой, по крайней мере, в большинстве работ. Возможно, детальная классификация способов, которые допустимы для распространения персональной информации, облегчит некоторые законные опасения насчет эффектов цифрового вторжения.

Ученый и писатель-фантаст Дэвид Брин (David Brin) в своей книге «Прозрачное общество» («The Transparent Society») говорит:

> Прозрачность подразумевает не проникновение в частную жизнь. Она предполагает возможность контролировать тех, кто может *вторгаться* в чужой внутренний мир. Право на личную жизнь – это спокойствие в доме и право на одиночество. Может раздражать, как много люди знают обо мне, но у меня нет права контролировать их умы. С другой стороны, меня сильно беспокоит, что другие *делают* по отношению ко мне и тем, кого я люблю. У каждого из нас есть право на место, где нас никто не сможет побеспокоить.[2]

Несмотря на огромные усилия и изощренные технологии, мы не можем контролировать распространение персональной информации. И мы часто хотим, чтобы информация стала общедоступной и послужила нашим целям или целям общества.

А еще нужны принципы учета случаев неправильного использования информации. Некоторые текущие разработки предполагают создание новой веб-технологии, в которой информация будет использоваться только по назначению, даже если попадет в чужие руки.[3] Возможно, инструменты классификации и выявления информационных связей могут быть модифицированы для ограничения нецелевого использования информации, попавшей в Интернет. Однако продолжается противостояние ограничения персональной информации и свободы слова:

---

[1] Д. Вайтцнер (D. Weitzner) «Beyond Secrecy: New Privacy Protection Strategies for Open Information Spaces» (За границами секретности: новые стратегии защиты персональных данных в открытых информационных пространствах), IEEE Internet Computing, сентябрь/октябрь 2007 года, *dig.csail.mit.edu/200/09/ieee-ic-beyond-secrecy-weitzner.html*.

[2] Дэвид Брин (David Brin) «The Transparent Society» (Прозрачное общество), Perseus Books, 1998, с. 334.

[3] Дэниел Вайтцнер, Харольд Абельсон, Тим Бернерс-Ли, Джоан Фейгенбаум, Джеймс Хендлер, Джеральд Джей Зуссман (Daniel J. Weitzner, Harold Abelson, Tim Berners-Lee, Joan Feigenbaum, James Hendler, and Gerald Jay Sussman) «Information Accountability» (Возможность учета информации), MIT CSAIL Technical Report, MIT-CSAIL-TR-2007-034 от 13 июня 2007 года.

мое право сказать правду о ком-то ограничено его правом на нераспространение информации, способной ему повредить. Таково реальное состояние права на неприкосновенность частной жизни, сильно потрепанного цифровым взрывом.

Включены постоянно

В воображаемом 1984 году технические средства всеобщего наблюдения могли быть отключены:

> Проходя мимо телекрана, О'Брайен вдруг словно вспомнил о чем-то. Он остановился и нажал выключатель на стене. Раздался щелчок. Голос смолк.
>
> Джулия тихонько взвизгнула от удивления. Уинстон, несмотря на панику, был настолько поражен, что не удержался и воскликнул:
>
> – Вы можете его выключить?!
>
> – Да, – сказал О'Брайен, – мы можем их выключать. Нам дано такое право... Да, все выключено. Мы одни.[1]

Иногда мы тоже можем и должны их выключить. Но, как правило, мы не хотим. Мы не хотим быть одни; мы хотим быть «на связи». Нам удобно быть в Сети, оставлять цифровые следы везде, где нас могут узнать по этим следам. Нам лень повторно набирать имя и адрес при возвращении на веб-сайт. Нам нравится, когда работники ресторана запоминают наше имя (а может, им напоминает имя база данных). Мы довольны возможностью купить виноград по цене 1 доллар 95 центов за фунт вместо 3 долларов 49 центов, при этом всего лишь позволяя супермаркету знать, где мы сделали покупку. Мы можем позволить оставить наблюдение за собой, потому что мы знаем, что наблюдение ведется и за преступниками. Наблюдают за ними. Наблюдают за нами.

Возможно, знание других о нас не так уж сильно беспокоит нас потому, что это привычный способ существования человечества: родовые общины и небольшие поселения, где знание всего друг о друге было вопросом выживания. Может быть, это врожденное свойство, сформировавшееся тысячелетия назад, до того как городская жизнь породила всеобщее отчуждение. И сегодня понятие частной жизни в маленьком провинциальном городке сильно отличается от такового в квартале Верхний Истсайд на Манхэттене.

Мы не знаем цены того, что мы все время «на связи». Добровольная раздача персональных данных так же опасна, как и властное ограничение личной свободы. Как остроумно подметил профессор Фано, право на неприкосновенность частной жизни допускает социальное экспериментирование – отклонения от норм общественного поведения, которые могут быть опасны для индивида в настоящем, но в прошлом

---

[1] «1984», часть 1, глава VIII.

могли быть основой прогрессивных общественных изменений. Будучи постоянно под наблюдением, мы обычно не пытаемся делать что-то выходящее за общепринятые рамки и можем остановиться в общественном развитии.

В большинстве случаев отключение происходит слишком поздно. Возможно, у нас когда-то была такая привилегия, но мы ее утратили. Нам придется решать свои проблемы иными способами.

Цифровая экспансия разбивает старые представления о том, кому что известно. Биты перемещаются быстро, недорого и множеством совершенных копий. Информация, которая в принципе считалась публичной – например, судебные протоколы, стоимость дома, истории в местном газетном листке, – теперь абсолютно общедоступна. Информация, которая в принципе считалась закрытой и почти никому не доступной – к примеру, медицинские записи и персональные фотографии – может получить широкое распространение из-за небрежности или злого умысла. Законы, деловая практика, социальные нормы не успевают за переменами.

Наиболее старый и надежный способ связи – письменный документ. Бумажные документы уступают дорогу электронным аналогам, с которых делают бумажные копии. Разве электронные документы во всем подобны бумажным? И да, и нет, и ошибочное понимание разницы может дорого обойтись. К обсуждению разницы мы сейчас и перейдем.

Глава 3 | Фантасмагории электронного мозга

Секреты и сюрпризы электронных документов

Компьютер знает о вас намного больше, чем показывает

4 марта 2005 итальянская журналистка Джулиана Сгрена была освобождена из багдадского плена, где ее удерживали заложницей в течение месяца. Когда автомобиль, предназначенный для обеспечения безопасности журналистки, приблизился к посту вооруженных сил США, американские солдаты открыли огонь. Джулиана Сгрена и водитель получили ранения, был убит агент итальянской разведки под прикрытием Никола Калипари.

Разгорелся яростный спор о причинах, по которым американские солдаты открыли огонь по автомобилю, в котором находились граждане дружественного государства и союзника по иракской военной кампании. Со стороны США поступили заявления о том, что автомобиль двигался на высокой скорости и не замедлил движения после предупредительных окликов. Итальянская сторона отвергла оба заявления. Этот случай вызвал дипломатическую напряженность между США и Италией, создав серьезные политические проблемы итальянскому премьер-министру.

Американская сторона предоставила отчет о произошедшем на 42 страницах, где высказывались суждения, оправдывающие американских солдат. Содержание отчета вызвало негодование итальянских представителей, и Италия срочно выпустила собственный отчет, с существенно отличающейся версией хода событий. Поскольку отчет США содержал закрытую военную информацию, перед широким распространением он был отредактирован (рис. 3.1).[1] Некоторые выражения были закрашены черным маркером, и в таком виде документ был размножен и его бумажные копии переданы репортерам. Но первоначально документ был создан в электронном виде. После редакции электронный доку-

[1] Полный и сокращенный варианты отчета можно найти во Всемирной паутине, например в Википедии: *en.wikisource.org/wiki/Calipari Report*.

мент был размещен на веб-сайте, который союзники использовали для предоставления военной информации СМИ. Поэтому любой из сотен миллионов пользователей Интернета мог прочитать отчет.[1]

(U) [redacted] has Direct Liaison Authorized (DIRLAUTH) to coordinate directly with [redacted] for security along Route Irish. This is the same level of coordination previously authorized by [redacted] Division to [redacted]. When executing DIRLAUTH, [redacted] directly coordinates an action with units internal or external to its command and keeps the [redacted] commander informed. The [redacted] TOC passes all coordination efforts through the [redacted] Brigade TOC to [redacted] JOC. (Annex 58C).

Рис. 3.1. *Абзац из страницы 10 отредактированного отчета США о факте смерти итальянского журналиста Николы Калипари. Информация, которая могла представлять интерес для противника, закрашена черным*

Источник: http://www.corriere.it/Media/Documenti/Classified.pdf, фрагмент страницы 10

И один пользователь, итальянский блоггер, внимательно изучив электронный документ, восстановил отредактированную информацию с помощью обычных офисных программ. Блоггер разместил полный текст отчета (рис. 3.2) на своем сайте. Раскрытая информация содержала сведения о расположении войск и средств оснащения, правила союзнических соглашений, процедуры взаимодействия войск союзников и другую интересную для противника информацию. Обнародование сведений не только представляло угрозу для войск, но и сильно смутило правительство США на пике трений между итальянскими и американскими властями.[2] Как такое вопиющее безобразие могло случиться в разгар самой высокотехнологичной войны в истории?

Бумажные и электронные документы в равной степени могут быть изучены, скопированы и сохранены. Но все же это разные вещи. Электронные документы легче исправлять, зато бумажные удобнее читать лежа в ванне. На самом деле, обозначение массива битов словом «документ» весьма условно. Заглянув за пределы видимого содержимого электронного документа, можно обнаружить удивительные и опасные вещи, как это случилось с вышеупомянутым отчетом.

Интерфейс под названием WYSIWYG (What You See Is What You Get – что видишь, то и получишь) пользуется заслуженной любовью со сто-

---

[1] Официальный сайт союзных сил: *www.mnf-iraq.com*. Отчет был убран сразу после обнаружения проблем с безопасностью, однако к этому времени он уже был скопирован.

[2] Гордон Хаусворт (Gordon Housworth) «Insurgents harvest secret NORORN materials from botched redaction of Nicola Calipari-Giuliana Sgrena incident report» (Повстанцы получили ценные разведданные из отчета Сгрена-Калипари), Intellectual Capital Group, *spaces.icgpartners.com/apps/discuss.asp?guid=25930D60E7294C459DB22915B37F3F46*.

(U) 1-76 FA has Direct Liaison Authorized (DIRLAUTH) to coordinate directly with 1-69 IN for security along Route Irish. This is the same level of coordination previously authorized by 1st Cavalry Division to 2-82 FA. When executing DIRLAUTH, 1-76 FA directly coordinates an action with units internal or external to its command and keeps the 31D commander informed. The 1-76 FA TOC passes all coordination efforts through the 4th Brigade TOC to 31D JOC. (Annex 58C).

Рис. 3.2. *Текст из рис. 3.1, где полностью убраны черные полосы*

Источник: http://www.corriere.it/Media/Documenti/Unclassified.doc

роны офисных сотрудников. Электронный документ отображается на мониторе так же, как впоследствии будет выглядеть бумажная распечатка. Так возникает заблуждение о том, что компьютер хранит множество маленьких копий изображений с экрана.

На самом деле, хранятся наборы кодов, которые интерпретируются в кранное изображение. Поэтому битовая метафора WYSIWYG не точна, а следовательно, опасна. Случай с отчетом о смерти Николы Калипари ясно показывает, что может случиться, если воспринимать эту метафору буквально. То, что авторы документа видели, разительно отличалось от того результата работы, который они получили.

Отчет делался с помощью программы, создающей файлы формата PDF. В таких программах бывает инструмент вроде Highlighter Tool (инструмент подсветки), играющий роль маркера, оставляющего на бумаге слабый след, сквозь который можно различить текст (рис. 3.3).

Кнопка инструмента Highlighter Tool обычно желтого цвета (цвет маркера Highlighter Tool), однако пользователь может задать другой цвет. Видимо, кто-то попытался использовать Highlighter Tool как инструмент редактирования, задав для него черный цвет и не зная о том, что видимое на экране и хранимое в документе – это две разные вещи.

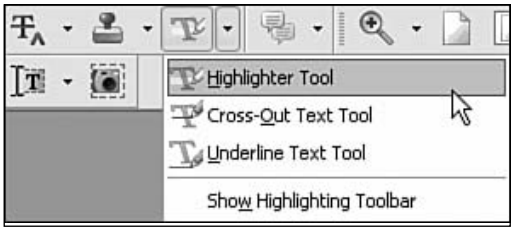


Рис. 3.3. *Инструмент Highlighter Tool в программе Adobe Acrobat. На экране инструмент оставляет желтый след, но с помощью команд меню можно задать любой другой цвет полосы*

Повторно публикуется с разрешения корпорации Adobe Systems Incorporated

Блоггер из Италии сообразил, что черные полосы наложены на текст инструментом Highlighter Tool черного цвета, при этом «замазанные» слова и выражения оставались в электронном документе. После этого открытия восстановить текст было просто.

Подобную ошибку несколькими годами раньше совершили две крупные газеты. 16 апреля 2000 года *New York Times* опубликовала статью о секретной попытке ЦРУ свергнуть иранское правительство в 1953 году.[1] Газета воспроизвела часть отчета ЦРУ, закрыв черными полосами имена сотрудников американской разведки в Иране. Статья появилась в Интернете в середине июня. К ней прилагались несколько страниц отчета разведки в виде документов PDF. Джон Янг, администратор раздела сайта, посвященного закрытым правительственным документам, удалил слои черных полос и открыл имена агентов ЦРУ. Возник спор об этичности и правомерности раскрытия имен, но дело было уже сделано, а документы с именами по-прежнему доступны в Интернете.[2]

Газета *Washington Post* совершила похожую ошибку в 2002 году, опубликовав статью о письме, оставленном вашингтонскими снайперами Джоном Алленом Мухаммадом и Джоном Ли Мальво. Как сообщалось на веб-сайте газеты, определенная информация была отредактирована способом, который был легко обойден любознательным читателем онлайн-издания (рис. 3.4).[3] Газета исправила промах, но недостаточно быстро для того, чтобы предотвратить копирование.[4]

Можно ли было защитить публикуемые документы в формате PDF от восстановления закрытого текста? Программа Adobe Acrobat содержит функцию безопасности с применением шифрования (см. главу 5), которая предотвращает изменение документа посторонними лицами при сохранении возможности просмотра документа. Возможно, создатели документа не знали о наличии такой функции, как и о коммерческом программном средстве Redax, которое правительственные агентства используют для редактирования текста документов, созданных в программе Adobe Acrobat.

---

1 *www.nytimes.com/library/world/mideast/041600iran-cia-index.html*

2 *cryptome.org/cia-iran.htm*

3 Серж Ф. Ковалеский, Сари Хорвиц (Serge F. Kovaleski and Sari Horwitz) «In letter, killer makes demands and threats» (Письмо киллера содержит требования и угрозы), *Washington Post* от 26 октября 2002, A14.

4 «Washington Post's scanned-to-PDF sniper letter more revealing than intended» (PDF-версия письма снайпера открывает больше, чем предполагалось), *PlanetPDF* от 26 октября 2002 года, *www.planetpdf.com/mainpage.asp?webpageid=2434*. Изображения со слайдов Стивена Дж. Мэрдока и Максимилиана Дорнсейфа (Steven J. Murdoch and Maximillian Dorn-seif) «Hidden data in Internet published documents» (Скрытые данные в интернет-документах), Кембриджский университет, 27 декабря 2004 года, *www.ccc.de/congress/2004/fahrplan/files/316-hidden-data-slides.pdf*.

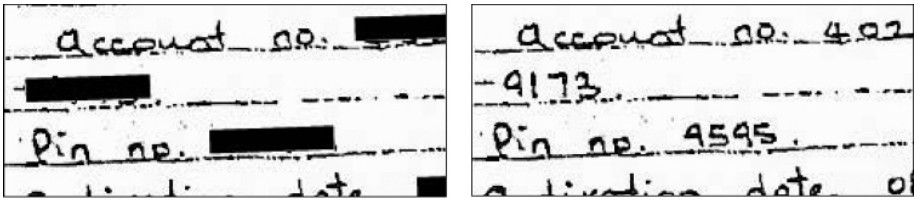


Рис. 3.4. *Письмо от вашингтонских снайперов. Слева – отредактированная версия с сайта газеты «Washington Post»; справа – оригинал с удаленными слоями черных полос*

Источник: веб-сайт газеты «Washington Post», скопированный на ***web.bham.ac.uk/forensic/news/02/sniper2.html***

Подлинные изображения, скопированные со слайда 29 файла: ***http://www.ccc.de/congress/2004/fahrplan/files/316-hidden-data-slides.pdf***

Более примитивный, но эффективный способ защиты состоит в том, чтобы распечатать документ с черными полосами в нужных местах, а потом отсканировать его. Результирующий файл будет содержать только сетку из черных и белых точек, утратив всю структурную информацию о тексте (названия шрифтов, значения отступов и так далее). Хотя скрытый таким образом текст действительно нельзя восстановить, данный метод достаточно неудобен.

Одно из достоинств форматированных текстовых документов, таких как файлы в формате PDF, – то, что они содержат не только оформление, но и собственно читаемый текст. В таком документе можно выполнять поиск по тексту, выделять и копировать фрагменты текста. Документ, превращенный в массив черных и белых точек, перестает быть текстом.

При печати и последующем сканировании теряется еще одна важная возможность. Документ становится бесполезен для программ, которые «озвучивают» текст для пользователей с нарушениями зрения. Специальные программы могут имитировать речь, «читая вслух» содержимое документа PDF, в том числе отчет США о смерти Калипари, но не сумеют распознать текст в отсканированном документе.

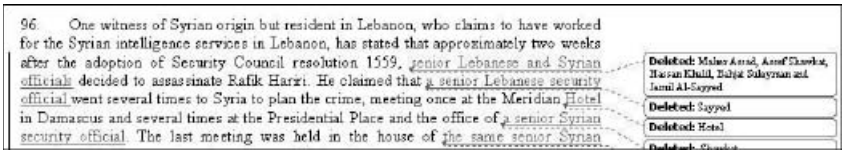
Внося исправления, не забывайте о том, что они сохраняются

В октябре 2005 года прокурор ООН Детлев Мелис подготовил для СМИ отчет о расследовании убийства бывшего ливанского премьер-министра Рафика Харири. Подозревали, что к подготовке убийства имеет отношение Сирия, но президент страны Башар Эль-Ассад отвергал все обвинения.

Прокурор Мелис сообщил, что отчет неокончательный[1], но есть «доказательства участия Ливана и Сирии». «Доказательством», которое было удалено из отчета, но восстановлено репортерами, получившими документ, было провокационное заявление о том, что брат президента Сирии и командир Республиканской гвардии Махер Ассад лично причастен к убийству.

В программе Microsoft Word есть функция «Исправления». Если она включена, то каждое изменение, внесенное в документ, записывается и хранится как часть документа, хотя в обычном режиме это не видно. Вместе с документом может путешествовать и история его создания: кто, когда и где внес изменения и какие именно. Также разные рецензенты могут добавлять свои комментарии, которые не появляются в конечном документе, но могут помочь донести их мысли до коллег по офису.

Конечно, для случайных читателей информация о стратегическом планировании не имеет ценности, но попадание содержимого правовых документов в руки противника может иметь катастрофические последствия. Удалить примечания из документа легко, но кто-то должен помнить о том, что это надо сделать! Прокурор ООН забыл о необходимости удалить историю исправлений из отчета в формате документа Word, и внимательный репортер смог прочитать скрытый текст (рис. 3.5). (Конечно, в делах Ближнего Востока нельзя быть слишком подозрительным. Некоторые подумали, что прокурор намеренно оставил текст в документе, как предупреждение Сирии о том, что он знает больше, чем говорит.)


96. One witness of Syrian origin but resident in Lebanon, who claims to have worked for the Syrian intelligence services in Lebanon, has stated that approximately two weeks after the adoption of Security Council resolution 1559, senior Lebanese and Syrian officials decided to assassinate Rafik Hariri. He claimed that a senior Lebanese security official went several times to Syria to plan the crime, meeting once at the Meridian Hotel in Damascus and several times at the Presidential Place and the office of a senior Syrian security official. The last meeting was held in the house of the same senior Syrian

Deleted: Maher Assad, Assef Shawkat, Hassan Khalil, Bahjat Suleyman and Jamil Al-Sayyed

Deleted: Sayyed

Deleted: Hotel

Рис. 3.5. *Фрагмент отчета ООН о расследовании убийства Рафика Харири. Первоначальный документ содержал сведения о том, что Махер Ассад и другие официальные лица причастны к убийству, но в готовом для СМИ документе их имена были заменены фразой «высшие официальные лица Сирии и Ливана»*

Источник: фрагмент отчета ООН, размещенного на веб-сайте газеты «Washington Post», www.washingtonpost.com/wp-srv/world/syria/mehlis.report.doc

---

[1] Джеймс Боун, Николас Блэнфорд (James Bone and Nicholas Blanford) «UN office doctored report on murder of Hariri» (ООН выпустила отчет об убийстве Харири), *Times* (Лондон) от 22 октября 2005 года; Майкл Янг (Michael Young) «Assad's dilemma» (Дилемма Ассада), *International Herald Tribune* от 28 октября 2005 года. Отчет доступен на веб-сайте *Washington Post*, *www.washingtonpost.com/wp-srv/world/syria/mehlis.report.doc*.

Отдельный пример проявления небрежности при редактировании документов подала корпорация SCO, заявившая, что другие корпорации нарушили ее права на интеллектуальную собственность. В начале 2004 года корпорация SCO подала жалобу в суд штата Мичиган на автопроизводителя Daimler Chrysler, заявляя, что им были нарушены положения лицензионного соглашения об использовании программного обеспечения SCO UNIX. Выяснилось, что в электронной версия заявления сохранилась история исправлений документа, открывающая любопытную информацию о планировании корпорацией SCO хода судебного процесса. В частности, из истории исправлений следовало, что до 11 часов 10 минут 18 февраля 2004 года корпорация SCO планировала возбудить иск против другой компании, Bank of America, направив его в федеральный, а не окружной суд, и к тому же за нарушение авторских прав, а не положений соглашения![1]

Служебная информация, сохраняемая в электронном документе

Электронный документ (к примеру, результат работы в текстовом процессоре) всегда содержит информацию *о самом себе* – так называемые *метаданные*. Самый очевидный пример метаданных – имя файла. Имя файла обладает малой степенью риска. К примеру, отправляя кому-либо файл, вложенный в сообщение электронной почты, вы понимаете, что получатель увидит имя файла прежде, чем его содержимое. Но почти всегда с файлом связано гораздо больше информации, чем одно лишь имя. Метаданные обычно содержат условное имя, ассоциированное с владельцем компьютера, а также даты и время создания и последнего изменения – это очень полезно, когда нужно узнать, получили ли вы старую или обновленную версию файла. Некоторые текстовые процессоры включают в документ информацию о версии, то есть запись о том, кто, когда и почему вносил изменения. Даже такая безобидная информация может представлять опасность, потому что обычно невидима. На рис. 3.6 из метаданных извлечена информация о военнослужащем, создавшем отредактированную версию отчета о смерти Николы Калипари.

Утечка информации об авторстве может иметь серьезные последствия. В 2003 году правительство Тони Блэра выпустило документ о содействии британского правительства действиям американских войск в Ираке. В документе было множество недостатков – значительные части текста были выдернуты и заменены доктринами тринадцатилетней давности. Проблему представляло то, что из готового файла, размещенного на официальном сайте офиса премьер-министра, не были убраны

[1] Стивен Шэнкланд, Скотт Ард (Stephen Shankland and Scott Ard) «Hidden text shows SCO prepped lawsuit against BofA» (Скрытый текст показывает, что SCO сфабриковала дело против BofA), *ZDNet* от 4 марта 2004 года, *news.zdnet.com/2100-3513_22-5170073.html*.

File name	sgrena_report.pdf
Document Type	PDF Document
File size	251072 bytes
Page size	8.5 x 11.0 inches
PDF version	1.4
Page count	42
Encryption	None
Modification Date	04/30/05
Title	I
Content Creator	Acrobat PDFMaker 6.0 for Word
PDF Producer	Acrobat Distiller 6.0 (Windows)
Creation Date	04/30/05
Author	richard.thelin

Рис. 3.6. *Часть метаданных из файла отчета о смерти Николы Калипари, полученная с помощью команды* ***Properties программы Adobe Acrobat Reader.*** *Видно, что автором документа является Ричард Телин и что он изменил файл в день его создания. Во время инцидента Ричард Телин состоял в морской пехоте США в звании подполковника*

Повторно публикуется с разрешения корпорации ***Adobe Systems Incorporated***

Редактирование метаданных

Метаданные могут помочь опровергнуть или подкрепить чьи-то утверждения. Предположим, ученик отправляет учителю домашнюю работу по электронной почте после срока сдачи. Ученик заявляет, что закончил работу точно в срок, но нарушения в работе Сети задержали доставку. Обман ученика может быть доказан, если он не знает, что одним из атрибутов документа является дата последнего изменения. Однако если ученик *знает* об этом атрибуте, то все, что ему нужно сделать, – это изменить показания часов на своем компьютере перед последним сохранением файла. Сетевое имя компьютера и другие атрибуты также могут быть изменены, что ограничивает судебную силу представления атрибутов документа в качестве доказательств.

цифровые отпечатки четырех гражданских служащих, составлявших документ. Как сообщалось в газете «Evening Standard of London», «всех этих сотрудников, занимающихся пропагандой, контролирует Алистер Кэмпбелл, глава пресс-службы Тони Блэра», хотя больше походило на то, что документ был разработан в министерстве иностранных дел.[1] «Иракское досье» вызвало серьезные волнения в парламенте.

[1] Джо Мерфи (Joe Murphy) «Campbell aide and team behind the dodgy dossier» (Помощник и команда Кэмпбелла стоят за иракским досье), *Evening Standard* (Лондон) от 25 июня 2003 года.

Проблемы от цифровых отпечатков в документах угрожают не только бизнесмену или высокопоставленному лицу. Отправляя по электронной почте сообщение с прикрепленным документом, скорее всего, вы отправляете и метаданные об авторе и времени создания или изменения этого документа. Также и с письмами, которые приходят к вам. Избавиться от метаданных можно, вставив текст документа в текст сообщения как большую цитату. Будьте внимательны и следите за тем, что вы отправляете!

Можно ли препятствовать утечке информации?

Даже во многих профессиональных организациях, не говоря об обычных семьях, немногие ответственные люди представляют себе опасность, заключенную в ошибочном использовании компьютерных технологий. Отчет о смерти Калипари был опубликован спустя пять лет после совершения аналогичной ошибки редакцией «New York Times». Как пользователи современных информационных технологий – то есть большинство образованных людей – могут своевременно узнать о новых методах защиты своих личных данных?

Не так-то легко предотвратить утечку важной информации, скрытой в документе и забытой его создателями или сохраненной в метаданных. В теории, учреждения должны разработать выходную инструкцию, по которой документы должны проходить «очистку» перед публикацией. Но в мире, объединенном информационными сетями, где электронная почта критически важный инструмент, очень трудно ввести такую инструкцию, не затормозив выполнение простейших действий. Другая серьезная мера состоит в отказе от программ, оставляющих в документах скрытые данные; так было сделано в Великобритании после скандала с «Иракским досье». Однако, отказываясь от них, теряешь возможность использования полезных программных функций. В-третьих, можно конвертировать форматированные документы (например ,файлы Microsoft Word) в форматы, сохраняющие меньше информации (например, Adobe PDF). Третья мера все же менее надежна, чем полная очистка от скрытых данных.[1]

Как минимум, необходимо серьезное обучение служащих. Предоставленное служащим программное обеспечение может вполне соответствовать их обязанностям, но многие полезные функции этих программ несут в себе риск использования. Нужно просто знать, каким образом вы редактируете свой документ. Люди зачастую рефлекторно нажимают одни и те же клавиши, запускают одни и те же функции и в первый, и в сотый раз, не думая о том, что сто первый раз может отличаться от предыдущих.

---

[1] Туомас Аура, Томас Кун, Майкл Роу (Tuomas Aura, Thomas A. Kuhn, and Michael Roe) «Scanning electronic documents for personally identifiable information» (Поиск персональной информации в электронных документах), WPES № 06 от 30 октября 2006 года, с. 41–49.

Представление, реальность и иллюзия

Бельгийский художник-сюрреалист Рене Магритт (René Magritte) на своей известной картине «The treachery of images» (Вероломство образов) (рис. 3.7) написал «Ceci n'est pas une pipe» (Это не трубка). Конечно, это не трубка – это образ трубки. С помощью кисти и краски художник оставил нам метафизическую шутку. Суть названия картины в том, что образ и реальный предмет не одно и то же.

Когда вы делаете снимок, внутри фотоаппарата происходит нечто, позволяющее впоследствии получить изображение. В цифровом фотоаппарате при съемке биты упорядочиваются в соответствии с некоторым шаблоном. Получается «представление» рисунка в памяти цифрового фотоаппарата. Если вы извлечете карту памяти и рассмотрите ее, то не увидите никакого изображения. Распечатав последовательность нолей и единиц цифровой информации из карты, вы также не получите изображения. Чтобы увидеть фотографию, нужно знать, *как* из последовательности битов собрать необходимую матрицу цветных точек. В области цифровой фотографии есть стандарты форматов хранения

Рис. 3.7. *Картина Рене Магритта с надписью по-французски «Это не трубка». Действительно, это всего лишь мазки краски, которые воображение смотрящего принимает за трубку, точно так же, как электронный документ – это всего лишь биты, которые пользователю видятся документом*

Музей искусств округа Лос-Анджелес. Картина приобретена на средства мистера и миссис Вильям Престон Харрисон, © Фотография, 2007, Музей искусств округа Лос-Анджелес, член Ассоциации музеев

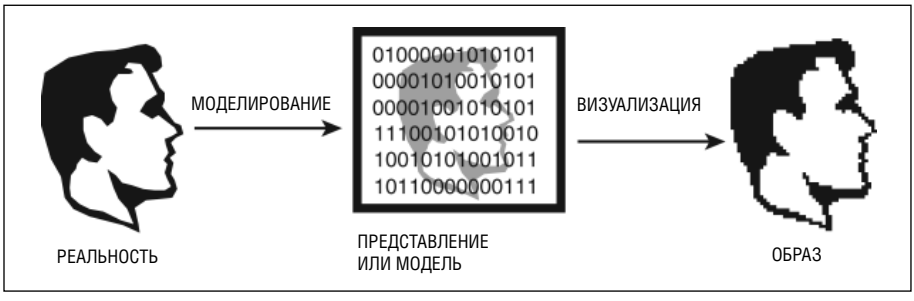


Рис. 3.8. *Схема двухэтапного получения цифрового фотоснимка. На первом этапе видимая реальность (сцена) переводится в поток битов с получением цифровой модели. На втором этапе модель визуализируется с получением образа (изображения). Модель можно хранить сколь угодно долго, копировать и обрабатывать на компьютере для улучшения качества получаемого изображения. Аналогичный принцип преобразования применяется как для видео-, так и для аудиоинформации*

изображений, поэтому снимки, сделанные различными фотоаппаратами, можно просматривать на разных компьютерах и распечатывать на разных принтерах.

Схема процесса получения цифровой фотографии показана на рис. 3.8. Некоторая внешняя реальность – сцена, видимая в объектив фотоаппарата, – некоторым образом кодируется в последовательность битов. Последовательность некоторым искусственным путем отражает часть видимой реальности. «Представление» реальности – некий фантом оригинала, отличный от него, но содержащий часть его свойств, достаточную для получения фотографии. Представление подчиняется определенным правилам, которые являются произвольными соглашениями, разработанными человеком. Правила общеприняты, что позволяет обмениваться фотографиями.

Результат представления фотографии в виде последовательности битов называется *моделью*, а сам процесс – *моделированием*. Изображение получается из модели путем *визуализации*. Визуализация происходит, когда поток битов модели отправляется на монитор или принтер. Визуализация «оживляет» фантом оригинала. Человеческий мозг считает, что воспринимает реальность, если, конечно, модель достаточно качественная. Некачественная модель – например, использующая слишком мало битов, – не может быть визуализирована в образ – изображение, очень похожее на оригинал.

Моделирование всегда основано на отбрасывании несущественной информации. Картина Рене Магритта не пахнет табаком, не имеет естественного налета, трубку нельзя повернуть и рассмотреть с других сторон. Не определив цель моделирования, невозможно определить, какая информация является существенной, а какая – нет. Тот, кто создает или визуализирует модель, может влиять на впечатление зрителя.

Процесс моделирования с последующим созданием образа используется не только в цифровой фотографии. Аналогично преобразуется звук при записи компакт-дисков или кодировании аудиозаписи в формат MP3. Представление музыки из цифровой модели выводится на звуковые колонки или наушники. Компакт-диски и формат MP3 используют разные методы моделирования; обычно звук на CD более качественный, хотя и требует больше битов.

Цифровые представления все же не полностью аналогичны реальным потокам информации; здесь проявляется разница между понятиями «аналоговый» и «цифровой». Аналоговый телефон представляет непрерывно изменяющийся звук с помощью непрерывно изменяющегося электрического сигнала (напряжение в телефонной линии изменяется «аналогично» реальному звуку), и Магритт так же плавно водил кистью по холсту, повторяя форму трубки. Переход от аналоговых технологий к цифровым в телефонии, телевидении, съемке, рентгеноскопии и других областях науки и техники, на первый взгляд, приводит к потере точности и простоты, присущих аналоговым приборам. Но благодаря высоким вычислительным мощностям современных цифровых устройств цифровое представление стало гораздо более гибким и полезным.

Примерно так же процессы оцифровки работают в ситуациях, когда *реальная составляющая отсутствует, потому что источник данных никогда не существовал в действительности*. Примером могут служить видеоигры, анимационные фильмы и виртуальные экскурсии по еще не построенным зданиям. В таких ситуациях нет первого этапа процесса, показанного на рис. 3.8. Модель получают не путем захвата части информации реальной сцены, а создают с «с чистого листа» – электронным пером художника или виртуальным чертежным инструментом системы автоматизированного проектирования.

Отсутствие в цифровом мире непосредственной связи между представлением и реальностью породило новые перспективы, риски и головоломки. Одним из первых триумфов цифровой обработки сигналов (области науки, посвященной компьютерной обработке цифровых представлений реальных объектов) стала очистка от щелчков и шумов старых записей великого певца Энрико Карузо.[1] Отфильтровать звуки старых записей и восстановить чистоту звучания голоса средствами старой аналоговой электроники было бы невозможно.

Разумеется, развитие цифрового «редактирования» не обошлось без «ложки дегтя». Программы-фоторедакторы, такие как Adobe Photoshop, позволяют подделывать снимки, используемые в суде в качестве доказательств.

---

[1] Томас Стокхэм (Thomas Stockham) «Restoration of Old Acoustic Recordings by means of Digital Signal Processing» (Восстановление старых звукозаписей средствами цифровой обработки сигналов), Общество аудиоинженеров, 1971 год.

Как удостовериться, что фотография не была отредактирована?

С помощью криптографических методов (обсуждаемых в главе 5) можно установить, что цифровая фотография не подвергалась обработке. Специальная камера получает цифровой ключ от системы верификации изображений, присоединяет к изображению «цифровую подпись» и выкладывает изображение и подпись в систему верификации. Система верификации обрабатывает полученное изображение с помощью ключа и сравнивает результат со значением подписи.[1] Система обеспечивает высокий уровень безопасности, потому что невозможно (вне зависимости от вычислительной мощности) создать изображение, обеспечивающее такую же подпись с тем же ключом.

Вряд ли анимационные фильмы наподобие «Истории игрушек» («Toy Story») в ближайшем будущем оставят актеров-людей без работы. Но как обществу реагировать на «синтетическую» детскую порнографию? В отличие от других форм порнографии, эта абсолютно противозаконна вследствие нанесения непоправимого вреда детям, подвергающимся насилию во время съемок. Но что делать, если показанные дети никогда не существовали в реальности, а появились лишь вследствие искусного владения средствами создания цифровой графики? В 1996 году Конгресс США объявил подобное вне закона: запрещается любое изображение, которое «является, кажется или по крайней мере похоже на явно сексуальное поведение».[2] Верховный суд отклонил этот закон на основании Первой поправки к Конституции США. Суд постановил, что принятый закон чрезмерно суров, и что подобные «синтетические» изображения, независимо от того, какие чувства они могут вызывать, являются результатом права на свободу слова.

В мире, где понятия истинной и искусственной реальности весьма расплывчаты, законы, сражаясь с проблемами общества, могут также угрожать праву на свободу выражения.

В данном случае под истинной реальностью понимается не собственно сюжет изображения. В главе 7 обсуждаются другие события, в которых общество борется за контроль над социальным злом, порожденным развитием информационных технологий. В мире, где понятия истинной и искусственной реальности весьма расплывчаты, законы,

[1] Камера Canon EOS-1 SLR. См. техническое руководство: *www.canon.com/technology/canon_tech/category/35mm.html*.

[2] Акт о недопущении детской порнографии 1996 года (Child Pornography Protection Act of 1996, CPPA), Кодекс законов США, том 18, 2256(8)(B).

сражаясь с проблемами общества, могут также угрожать праву на свободу выражения.

Что есть правильное представление

На рис. 3.9 изображена страница из Келлской книги, одного из шедевров средневекового оформительского искусства. Келлская книга была создана примерно в 800 году в ирландском монастыре. Страница содержит несколько латинских слов, украшенных сложным орнаментом и фигурами людей и животных. Книга насчитывает несколько сотен страниц, но оформление ни одной из них не повторяется. Искусные узоры на этой странице окружают всего 21 букву (рис. 3.10).

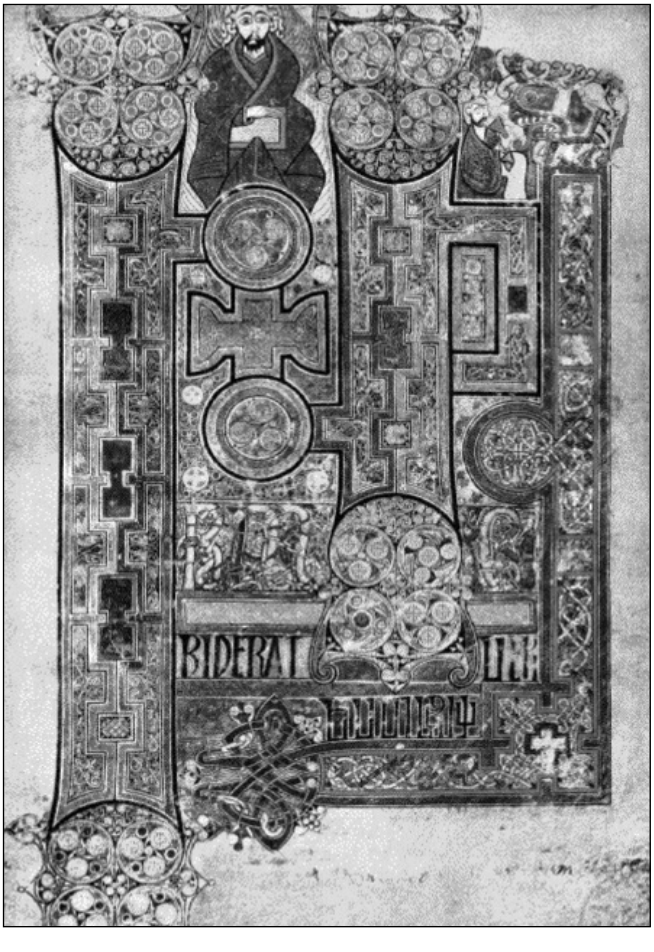


Рис. 3.9. *Начальная страница Евангелия от Иоанна из Келлской книги*

© Тринити-колледж, Дублин, Ирландия

```
IN PRINCIPIO ERAT VERBUM
```

Рис. 3.10. *Латинское начало Евангелия от Иоанна («В начале было слово»). В Келлской книге наиболее четко видно слово* ***ERAT слева от центра на расстоянии в четверть страницы снизу***

Содержат ли эти два изображения одинаковую информацию? Ответ зависит от того, что вы хотели записать. Если единственным важным элементом является латинская фраза, то оба представления в равной степени хороши, хотя прочитать второе гораздо легче. Но при создании Келлской книги значения имели не только слова. Книга является одним из величайших образцов западного художественного искусства и техники исполнения.

Изображение страницы с рис. 3.9 создано на основе прямоугольной сетки, каждая ячейка которой содержит информацию о цвете (рис. 3.11). Для получения сетки страница сканируется ряд за рядом, каждый из которых состоит из небольших квадратных элементов изображения – пикселов (picture elements, pixels). Изображение на основе прямоугольной сетки пикселов называется *растровым*, или *битовой картой*. Структура такого изображения соответствует структуре компьютерного экрана или цифрового телевизора. Экраны таких устройств также поделены на множество отдельных пикселов – чем меньше размер и больше количество пикселов, тем выше качество «картинки» и цена устройства.

А как в компьютере представлен простой текст на латинице, изображенный на рис. 3.10? Стандартная кодировка для латиницы, известная как Американский стандартный код для обмена информацией (American Standard Code for Information Interchange, ASCII), присваивает каждому символу отдельную восьмибитную последовательность (8 бит = 1 байт). Например, A = 01000001, a = 01100001, $ = 00100100 и 7 = 00110111.

Цифровые камеры и мегапикселы

Мегапикселы (миллион пикселов) – стандартная единица измерения для оценки качества цифровой камеры. Если камера захватывает малое количество мегапикселов, хороших фотографий не получится. Если мегапикселов достаточно, но у камеры плохие линзы, результат будет не лучше[1] – вы просто получите более детальное размытое изображение!

[1] Дэвид Пог (David Pogue) «Breaking the myth of megapixels» (Разрушение мифа о мегапикселах), *New York Times* от 8 февраля 2007 года.

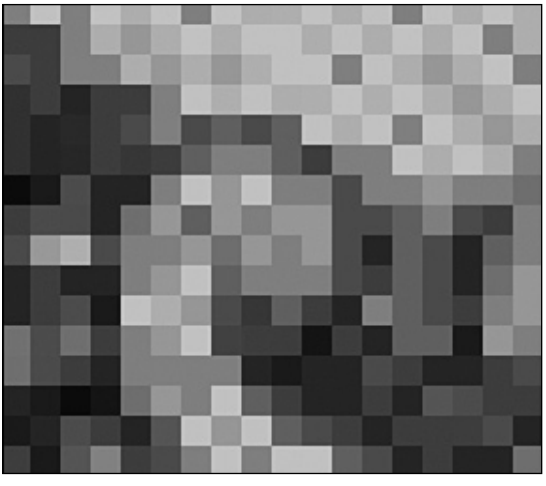


Рис. 3.11. *Увеличенный фрагмент отсканированной начальной страницы Евангелия от Иоанна из Келлской книги*

© Тринити-колледж, Дублин, Ирландия

01001001 01001110 00100000 01010000
01010010 01001001 01001110 01000011
01001001 01010000 01001001 01001111
00100000 01000101 01010010 01000001
01010100 00100000 01010110 01000101
01010010 01000010 01010101 01001101

Рис. 3.12. *Фраза «IN PRINCIPIO ERAT VERBUM», представленная в ASCII-коде*

Выражение 7 = 00110111 означает, что битовый код для представления символа «7» в текстовой строке равен 00110111. Символ пробела также имеет свой код: 00100000. На рис. 3.12 показана фраза «IN PRINCIPIO ERAT VERBUM», представленная в ASCII-коде в виде последовательности из 24 байтов (или 192 бит). На рисунке последовательность битов поделена на порции по 8 бит (по 1 байту) для облегчения чтения, но в компьютере биты расположены просто один за другим.

Таким образом, байт 01001001 соответствует символу «I». Это верно не всегда. Последовательностью битов представляют не только текстовые строки. Тот же байт 01001001, будучи интерпретирован как двоичное целое число, представляет 73. Компьютер не может знать, что на самом деле представляет собой байт 01001001, – может, это степень насыщен-

ности цвета. Компьютер может правильно интерпретировать битовую строку, только если ему известно соглашение, использованное при создании документа, то есть способ интерпретации содержимого файла.

Значение битовой строки зависит от принятого соглашения. Такие соглашения совершенно произвольны. Код символа «I» может быть и таким: 11000101, и любым другим. Когда соглашения принимаются многими в силу широты распространения и экономической целесообразности, они приобретают силу юридических документов. В настоящее время миллионы компьютеров считают, что код 01001001 в текстовой строке означает символ «I», и такое взаимное соглашение делает возможным повсеместный обмен информацией.

Расширения имен файлов

Три (как правило) символа после точки в конце имени файла указывают на способ интерпретации его содержимого. Некоторые расширения:

.doc – документ Microsoft Word

.odt – текстовый документ OpenDocument

.ppt – презентация Microsoft PowerPoint

.ods – электронная таблица OpenDocument

.pdf – документ Adobe Portable Document Format

.exe – исполняемый файл (программа)

.gif – графический файл Graphics Interchange Format (цветовая палитра не более 256 цветов)

.jpg – графический файл JPEG (стандарт организации Joint Photographic Experts Group)

.mpg – видеофайл MPEG (стандарт организации Moving Picture Experts Group)

Формат документа является ключом к созданию представления в виде воспринимаемого человеком документа. Если программа ошибочно распознает формат, то на выходе получается бессмыслица. Если на компьютере нет программы, способной обработать некоторый формат, то открыть документ этого формата на данном компьютере невозможно.

Какой способ представления документа лучше, растровый или в виде ASCII-кодов? Ответ зависит от предназначения документа. Для представления картины со множеством теней и оттенков цвета нет ничего лучше растровой сетки, при условии, что каждый пиксел содержит информацию о достаточно маленькой точке и что самих пикселов дос-

таточно. Однако даже привычному человеку будет нелегко разыскать буквы на рис. 3.9, а уж для компьютерной программы это почти невозможно. Легко читать и осуществлять поиск по тексту в файле, формат которого основан на ASCII-кодах, таком как PDF.

Но документ формата PDF может содержать много больше, чем ASCII-коды. Документ PDF может включать информацию о шрифтах, цвете текста и фона, размерах и точной позиции символов. Программное обеспечение, создающее файлы формата PDF, служит для создания высококачественных полиграфических документов, таких как тот, что вы сейчас читаете. Другими словами, PDF является *языком разметки страниц* и описывает важные типографские свойства видимых элементов документа. Для полностью графических документов следует использовать графический формат, например JPG. Сложный документ PDF, описывающий страницы вроде этой, комбинирует текст и графику.

Снижение количества данных (в том числе без потери информации)

Давайте еще раз взглянем на изображение страницы Келлской книги (см. рис. 3.9) и увеличенный фрагмент изображения (рис. 3.11). Файл изображения имеет размеры в 463 пиксела в ширину и 651 пиксел в высоту, итого около 300 тысяч пикселов. Размер реальной страницы 10 на 13 дюймов, следовательно растровое изображение содержит около 50 пикселов на каждый дюйм страницы. Этого недостаточно для отображения всего богатства деталей изображения – на рис. 3.11 должна была быть видна голова животного из верхнего правого угла страницы. При сканировании было потеряно множество деталей; специалисты называют это «недостаточным разрешением». Сканирующее устройство «разрешает» непрерывную картинку в дискретную сетку точек, и, в данном случае, частота точек (графическое разрешение) слишком мала, чтобы передать все детали, видимые невооруженным глазом.

Естественно, для получения более детального изображения необходимо увеличить разрешение сканирования, то есть число пикселов на дюйм. На рис. 3.13 показано, как качество изображения улучшается с увеличением разрешения. Отдельный пиксел каждого изображения содержит информацию о «среднем» цвете оригинала.

За высокое разрешение приходится платить. Чем больше пикселов в изображении, тем больше компьютерной памяти требуется для его хранения. При удвоении разрешения объем необходимой для хранения памяти увеличится вчетверо, так как удвоение выполняется и по вертикали, и по горизонтали. Популярные программы для более экономичного хранения графических файлов используют технологии сжатия. Есть два класса технологий сжатия: без потерь информации (lossless compression) и с потерями (lossy compression). Сжатие без потерь при распаковке дает результат, неотличимый от оригинала. Сжа-

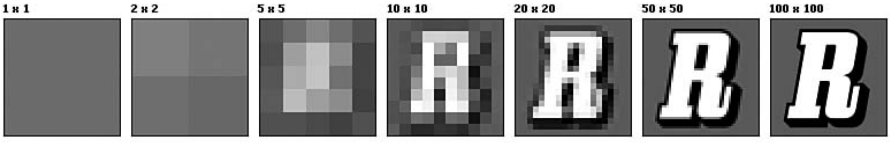


Рис. 3.13. *Изображение при различных значениях разрешения от 1×1 до 100×100 пикселов. Квадратный блок пикселов одного цвета можно представить более компактно, чем множеством одинаковых пикселов, – кодировать только один пиксел и указывать количество*

Взято из Википедии, ***en.wikipedia.org/wiki/Image:Resolution_illustration.png***

тие с потерями создает изображение, близкое к оригиналу, путем отбрасывания части графической информации, что человеческий глаз может заметить или нет.

Один из методов сжатия графики без потерь основан на том факте, что в большинстве изображений цвета многих соседних пикселов совпадают или, используя соответствующую терминологию, имеют *пространственную связность*. Если внимательно рассмотреть изображения посередине и справа, то можно заметить, например, что на изображении с разрешением 100×100 левый верхний квадрат 10×10 содержит пикселы одного цвета; нет необходимости повторять 24-битные значения 100 раз. Средства сжатия позволяют записать это в файл в краткой форме, следовательно, размер файла уменьшится.

В зависимости от ваших целей может иметь смысл применить метод сжатия с потерями. К примеру, изображение на телеэкране мелькает так быстро, что уследить за всеми пикселами невозможно. Но в некоторых случаях приемлемо только сжатие без потерь. Если вы хотите сохранить в цифровом архиве фильм Запрудера об убийстве президента Кеннеди, целесообразно создать копию без потерь информации с высоким разрешением. А отправляя рисунок на печать на принтер с низким разрешением печати, уместно сэкономить память за счет сжатия с потерями.

Сжатие звука

Формат MP3 – метод сжатия звуковых файлов с потерей информации. При сжатии используется множество приемов, позволяющих получать файлы небольшого размера. К примеру, человеческое ухо плохо различает низкие частоты в стереофоническом режиме, и эта составляющая звука кодируется в монофоническую, а при воспроизведении подается в оба динамика, в то время как высокочастотные звуки кодируются в стерео. Качество звука, обеспечиваемое форматом MP3, в большинстве случаев приемлемо, однако при чутком слухе потерю качества можно заметить.

Рождение и гибель технологий

Цифровая революция стала возможной благодаря тому, что емкость микросхем памяти нарастала по закону Мура. Появилась возможность хранить оцифрованные изображения и звуки с качеством, превосходящим качество аналоговых вариантов. Кроме того, снижение цен позволило включить карты памяти в список потребительских товаров. Однако дело не только в электронике. Цифровые камеры и HD-телевизоры с более чем одним мегабайтом на кадр могли бы еще долго оставаться редкостью. *Мегабайт* – это около миллиона байтов, слишком много для одного кадра. Революции способствовало появление новых алгоритмов обработки и новых, быстрых и дешевых микропроцессоров, способных эффективно выполнять данные алгоритмы.

Например, технология видеосжатия использует и пространственную, и *временную связность*. Как правило, соседние кадры не очень сильно отличаются друг от друга, поэтому нет смысла передавать весь следующий кадр, особенно, учитывая, что это надо делать 30 раз в секунду. В принципе, можно передать только отличия от предыдущего кадра. Если на экране изображается женщина, гуляющая по неподвижному ландшафту, то необходимо передать только новое изображение женщины и часть изображения ландшафта, появившегося за ней, и, если это возможно и целесообразно, пересчитать предыдущий кадр с учетом новой информации. На прием отличий и расчет нового кадра у алгоритма есть только одна тридцатая доля секунды.

Цифровое видео не могло бы получить развития, если бы не беспрецедентный рост вычислительной мощи при одновременном снижении цен на компьютеры. Алгоритмы распаковки встроены в настольные фотопринтеры и ресиверы кабельного телевидения, кремниевые микросхемы которых выполняют вычисления быстрее, чем самые быстрые настольные компьютеры еще несколько лет назад. Сжатые данные можно быстрее передать по кабелю или через спутник. Производительность кабельных ресиверов и цифровых телевизоров в настоящее время достаточно велика, чтобы восстановить изображение по данным, содержащим только отличия между кадрами. Вычисления – сила!

По контрасту, одна из причин ухода компакт-дисков со сцены носителей музыки – недостаточная емкость. Когда формат CD был стандартизирован, электроника для распаковки сжатого звука была чрезмерно дорогой для установки в массовых устройствах, поэтому данные хранились в несжатой форме. Сила плеера Apple iPod не только в высокой емкости и малом размере его накопителя, но и в производительности процессора, восстанавливающего музыку из модели.

Рождение новых технологий влечет за собой гибель старых. Цифровые фотоаппараты уничтожают пленочную фотографию; аналоговые телевизоры уступают место цифровым; грампластинки были потеснены кассетными лентами, которые сменились компакт-дисками, а теперь

и компакт-диски освобождают дорогу цифровым музыкальным плеерам с их форматами сжатия звука.

Переходные периоды, когда новые многообещающие технологии только начинают теснить популярные старые, часто бывают отмечены всплесками усилий, не всегда прогрессивных. Фирмы, владеющие старыми технологиями, иногда вводят инновации, но обкатанное производство трудно перенастроить. В худшем случае, пытаясь удержаться на рынке, они начинают вставлять палки в колеса прогресса. Например, они могут распускать слухи о мнимом вреде новых технологий или о высоких затратах на обновление.

Форматы данных, всего лишь соглашения для обмена информацией, могут быть причиной серьезных разногласий, если смена формата угрожает бизнесу или правящей партии, что ощутило на себе правительство Массачусетса, когда попыталось изменить формат своих документов. Случай с переходом на формат OpenDocument показывает, как трудны могут быть перемены в цифровом мире, хотя иногда кажется, что перемены происходят ежедневно.

Форматы данных как общественная собственность

Интернет ничей, и в то же время им владеют все пользователи. Ни одно правительство не может контролировать всю систему; в США федеральное правительство контролирует только компьютеры правительственных агентств. Когда вы скачиваете веб-страницу на свой компьютер, она может пройти через узлы нескольких (возможно, десятков) частных коммуникационных компаний, располагающихся на маршруте от веб-сервера к вам.

Гибкая и динамичная конфигурация компьютеров и коммуникационных каналов возможна потому, что Интернет по сути опирается не на аппаратуру связи, а на коммуникационные протоколы – соглашения, которые компьютеры используют для взаимного обмена битами (см. приложение). Базовый протокол Интернета обозначается аббревиатурой IP. Интернет смог быстро вырасти по той причине, что описания стандартов IP и других протоколов стали общедоступными. Любой программист имел право создавать производные протоколы, каждый из которых имел шанс получить статус стандартного в случае одобрения сетевым сообществом. Самый важный протокол на основе IP обозначается аббревиатурой TCP. Протокол TCP используется веб-приложениями и электронной почтой для надежной доставки сообщений; пара базовых протоколов обозначается как TCP/IP. Интернет не мог бы так динамично развиваться, если бы опирался на «закрытые» (то есть находящиеся в частном владении) протоколы, имевшие место в начале развития компьютерных сетей.

Так было не всегда. Двадцать или тридцать лет назад все ведущие производители компьютерного оборудования – IBM, DEC, Novell и Apple –

использовали собственные коммуникационные протоколы. Для установки связи между компьютерами разных компаний требовалось приложить изрядные усилия, и каждая компания надеялась, что весь остальной мир примет за стандарт именно ее протоколы. Протокол TCP/IP стал стандартом, потому что правительственные агентства США настаивали на его использовании в исследованиях, спонсируемых властями, – сеть ARPANET работала на Департамент обороны, а сеть NSFnet использовалась Национальным научным фондом (National Science Foundation, NSF). Поддержка протокола TCP/IP входила в программное обеспечение операционной системы Berkeley UNIX, разработка которой поддерживалась федеральными грантами и которая широко использовалась в университетах. Небольшие компании быстро научились задействовать TCP/IP для своих целей; большие компании адаптировались медленнее. Интернет со всем своим богатством сервисов и производителей не мог бы развиться и упрочиться, если бы не взаимное упорство ведущих производителей – в этом смысле все они проиграли, несмотря на то что их коммуникационные решения во многом превосходили ранние реализации TCP/IP.

Downloading и uploading[1]

Исторически Интернет воспринимается как состоящий из мощных корпоративных серверов, расположенных «над» домашними персональными компьютерами. Так что получение материалов с сервера называется downloading (от down – англ. вниз), а когда данные передаются от вашего компьютера к серверу, это называется uploading (от up – англ. вверх). Многие персональные компьютеры сегодня настолько мощны, что сравнения «выше» и «ниже» не всегда уместны, но сами выражения закрепились в языке. См. также Приложение и описание технологии peer-to-peer в главе 6.

Стандарты на форматы файлов сегодня тоже на распутье. Растет беспокойство о рисках стандартизации коммерческих закрытых форматов. Предполагается, что общество получит лучшее обслуживание и безопасность при хранении документов в файлах общедоступных форматов, проверенных организациями по стандартизации, чем при использовании форматов, привязанных к коммерческим пакетам программ. Однако *де-факто стандартом* хранения текстовых документов является коммерческий формат DOC программы Microsoft Word.

[1] Downloading – загрузка («закачка») файла из Интернета, uploading – загрузка файла на удаленный сервер в Интернете (действие, также называемое выкладыванием). – *Прим. перев.*

Формат DOC – коммерческая закрытая разработка корпорации Microsoft. Детали формата в настоящее время опубликованы, но корпорация сохраняет за собой право в любой момент изменить формат без уведомления. И это происходит с завидной регулярностью, с целью усовершенствования программного обеспечения, что порождает проблемы несовместимости с уже существующими документами. Документ, созданный в версии программы Word 2007 не может быть обработан программой Word 2003 без специального программного дополнения, так что даже пользователи Microsoft Office рискуют столкнуться с проблемами несовместимости.[1] Корпорация Microsoft не исключает возможность для других разработчиков использовать ее форматы, но разработчики сильно рискуют, полагаясь на формат, который не могут контролировать.

В крупной организации стоимость лицензирования программ Microsoft Office для тысяч компьютеров может исчисляться миллионами долларов. С целью создания атмосферы здоровой конкуренции Евросоюз в 2004 году ввел в обращение между правительствами и представителями бизнеса ЕС формат OpenDocument Format (ODF). Благодаря формату ODF множество компаний смогли выйти на рынок и иметь возможность читать документы, созданные программами различных разработчиков.

В сентябре 2005 года правительство Массачусетса решило поддержать инициативу ЕС. Предложение исходило от сторонника программного обеспечения с открытым исходным кодом, директора департамента информационных технологий Питера Куинна. Было официально заявлено, что в течение 15 месяцев все правительственные документы должны быть созданы или конвертированы в ODF. Это решение затрагивало около 50 тысяч правительственных компьютеров. Предполагалось сэкономить около 45 миллионов долларов. Но Эрик Крисс, правительственный секретарь по управлению и финансам, заявил, что выигрыш заключался не только в деньгах: публичные документы являются общественной собственностью и доступ к ним не должен находиться в зависимости от одной частной корпорации.

Корпорация Microsoft нашла, чем возразить.[2] Адвокаты корпорации выдвинули аргумент о том, что на данный момент не существует программного обеспечения, способного адекватно заменить ее программы. Кроме того, адвокаты сослались на уже заключенные контракты корпорации и правительства на сроки, превышающие дату конца перехода на формат ODF. Таким образом, принятие нового формата

---

[1] См., например, Шен Уэнг (Shan Wang) «New ‘Word’ frustrates users» (Новый Word раздражает пользователей), *Harvard Crimson* от 26 ноября 2007 года.

[2] Роберт Вейсман (Robert Weisman) «Microsoft fights bid to drop Office software» (Microsoft сопротивляется попыткам заменить Office), *Boston Globe* от 14 сентября 2005 года.

может являться нарушением соглашения и обойдется правительству в круглую сумму. «Если подобное предложение будет принято, то уровень затрат правительства, граждан и бизнеса Массачусетса сможет сравниться только со степенью неразберихи и несовместимости, которые за этим последуют, – ответил секретарь Крисс. – Вопрос состоит в том, обязано ли правительство штата удостовериться, что ко всем публичным документам можно будет обеспечить всеобщий доступ, не ограниченный ни патентами, ни лицензиями, ни другими техническими трудностями. Мы отвечаем, что обязано, это наш долг. Корпорация Microsoft заявляет свое несогласие, желая, чтобы весь мир использовал ее закрытые форматы». Спор затих, но давление усилилось. Ставки были высоки для корпорации: примеру Массачусетса могли последовать другие штаты.

Три месяца спустя ни Эрик Крисс, ни Питер Куинн уже не работали в правительстве. Крисс вернулся в частный сектор, как и планировал до получения работы в правительстве. Газета *Boston Globe* опубликовала результаты исследования расходов Куинна на путешествия, но правительство оставило Куинна вне подозрений. Устав от клеветы, под огнем противников решения перехода на открытые стандарты, лишенный поддержки Крисса, 24 декабря Куинн объявил о своей отставке. Куинн подозревал, что за расследованием *Boston Globe* и сопротивлением законодательной власти инициативе по переходу на открытые стандарты стояли «деньги Microsoft и ее лоббистская машина».[1]

Срок перехода правительства Массачусетса на формат OpenDocument давно вышел, но осенью 2007 года на веб-сайте правительства все еще сообщалось, что переход состоится в будущем. Как разъяснили официальные лица, офисные приложения корпорации Microsoft в скором времени приобретут функции чтения и записи файлов в формате OpenDocument, поэтому переход не отразится на лидирующем положении Microsoft Office по отношению к другим офисным пакетам. Кроме того, другие разработчики не смогут предложить свои офисные решения до тех пор, пока «характеристики программ не смогут сравниться или превзойти соответствующие характеристики текущего офисного пакета»[2], то есть пакета Microsoft Office. Вплоть до настоящего времени корпорация Microsoft лидирует в игре несмотря на все усилия правительства вырвать из частных рук форматы публичных документов.

Решение о принятии того или иного формата – часть бизнеса с многомиллиардным оборотом. Как во всех больших сделках, вопрос решают деньги и голоса политиков, истина скрывается за обещаниями, а вся тяжесть решения ложится на плечи общества.

---

[1] *www.groklaw.net/article.php?story=20060123132416703*

[2] Веб-сайт департамента информационных технологий правительства штата Массачусетс, страница, посвященная формату OpenDocument.

OpenDocument, открытый исходный код и бесплатность

Эти три концепции нацелены, по крайней мере отчасти, на снижение роста монополий разработчиков программ. OpenDocument (сайт opendocument.xml.org) – это открытый формат и стандарт для файлов документов. Несколько ведущих корпораций предприняли соответствующие усилия и обещали не преследовать за нарушение права интеллектуальной собственности сторонних разработчиков программ, использующих данные стандарты. Open source (открытый исходный код, сайт *opensource.org*) – это методология разработки программного обеспечения, концентрирующая отдельные усилия разработчиков и тестеров для скорейшего создания качественных программ. На сайте *openoffice.org* можно найти полноценный набор офисных приложений, доступный бесплатно. Бесплатное, свободно распространяемое (free) программное обеспечение – «свободное означает свободу, а не халяву» (сайты *www.fsf.org, www.gnu.org*) – «предоставляет пользователям возможность свободно использовать, копировать, распространять, изучать, изменять и улучшать программное обеспечение».

Изображения скрывают информацию

Проблемы, вызываемые содержимым текстовых документов, обычно связаны с небрежностью или неосторожностью авторов. Графические изображения предоставляют неограниченные возможности для намеренного скрытия информации от случайных наблюдателей или для обхода программной защиты от спама.

Война со спамом

Многие часто получают письма, подобные таким: *«Меня зовут мисс Фаатин Рахман, я единственная дочь покойной миссис Хелен Рахман. Адрес: Рю 142 Маркори, Абиджан, Кот-д'Ивуар, Западная Африка. Мне 20 лет. Я потеряла своих родителей, но у меня осталось наследство от моей покойной матери. Мои родители были богатые фермеры и торговцы какао. После смерти моего отца мать долго вела его бизнес, но ее отравили партнеры и она умерла... Я прошу вас помочь мне: переведите на безопасный счет в банке...»*

Если вы получили подобное сообщение, ни в коем случае не отвечайте и не переводите деньги. Они навсегда утекут с вашего счета. Многие люди знают, что это обман. Однако нежелательная массовая почтовая

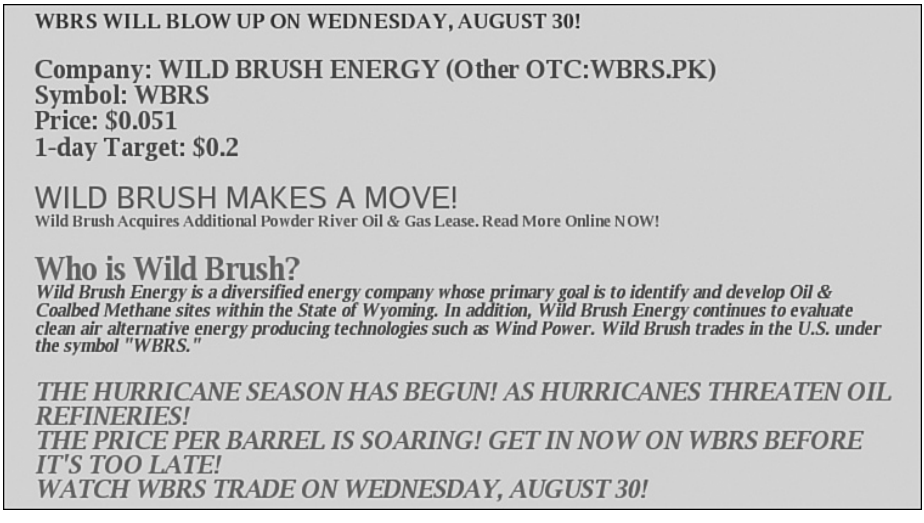


Рис. 3.14. *Графический спам, полученный одним из авторов книги. Хотя спам выглядит как текст, для компьютера это такое же изображение, как цифровая фотография. Спам-фильтр в данном случае бесполезен, так как не может выделить текст из рисунка*

рассылка (спам) обходится так дешево, что достаточно одного отклика на миллион, чтобы обеспечить спамеру безбедную жизнь.

Программы типа «спам-фильтр» отслеживают сообщения, подобные вышеприведенному, и удаляют их еще до того, как вы их прочтете. У спама обычно есть признаки, по которым его легко распознать с минимальным риском ошибочного удаления банковской корреспонденции или переписки с реальными африканскими друзьями.

Но спамеры совершенствуют свои методы. Многие люди получают сообщения электронной почты, подобные показанному на рис. 3.14. Спам-фильтр не обнаружил и не удалил спам. Почему?

Программы для обработки текстов сохраняют в файлах не только полиграфическую информацию (шрифт, цвет, размер символов и др.), но и собственно текст – **ASCII-коды с**имволов. Именно наличие **ASCII**-кодов позволяет редактировать текстовые строки, осуществлять поиск и выполнять другие операции с текстом. Когда пользователь наводит курсор на изображение символа на экране, программа устанавливает соответствие изображения символа и его кода в файле документа. Коды, в свою очередь, визуализируются на экране, как изображения символов.

Но то, что вы видите на экране алфавитный символ, не всегда означает, что изображение символа получено путем визуализации соответствующего **ASCII-кода. Цифровая фотография текста может выглядеть** совершенно так же. Это два разных представления одной информации.

И поскольку средствами спам-фильтра выделить текст из фотографии невозможно, в войне между разработчиками фильтров и спамерами пока побеждают последние. Спам, изображенный на рис. 3.14, был сохранен в виде графического файла. Поскольку текст такого сообщения образован расположением цветных пикселов, а не строкой ASCII-кодов, подобный спам обходит защиту всех фильтров, известных авторам книги!

Проблема конвертирования растровой графики в ASCII-текст называется *распознаванием символов*. Если оригинальный документ напечатан на бумаге, говорят об *оптическом распознавании символов* (optical character recognition, OCR). Сканированием получают растровое изображение, а затем алгоритм распознавания преобразует его в последовательность кодов символов. Если оригинальный документ напечатан стандартным шрифтом и не особо испачкан пятнами или кляксами тонера, то современное программное обеспечение для распознавания достаточно легко справится с работой. Программы распознавания символов прилагаются ко многим современным популярным моделям сканеров и многофункциональных устройств (объединяющих сканер, принтер или фотопринтер, копир и факс). Можно надеяться, что по мере усовершенствования и распространения алгоритмов распознавания фильтры нового поколения научатся обнаруживать спам, пример которого показан на рис. 3.14.

Алгоритмы OCR и спам иллюстрируют общую проблему. Представление определяет возможности манипуляции данными. В теории многие представления эквивалентны. Но на практике тайны форматов и вычислительные затраты на их конвертирование форматов могут снизить полезность самих данных.

Скрытие информации от неискушенного наблюдателя

Во время Первой мировой войны немецкое посольство в США отправило из Вашингтона в Берлин сообщение, которое начиналось так: «PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE». Американская разведка читала все немецкие телеграммы; эта могла показаться достаточно безобидной. Однако первые буквы слов образовывали слово «PERSHING» (название американского военного корабля). Продолжая читать телеграмму (обсуждающую президентское эмбарго), можно было получить полную фразу: «PERSHING SAILS FROM N.Y. JUNE 1» («PERSHING» отплывает из Нью-Йорка 1 июня»).[1]

Искусство незаметного скрытия тайных сообщений называется *стеганографией*. Стеганография отличается от *криптографии* (шифрования), искусства создания недешифруемых сообщений. Предположим, Алиса отправляет зашифрованное (средствами криптографии) письмо Бобу. Некто

[1] David Kahn «The Codebreakers», Scribner, 1996. Русский перевод: Дэвид Кан «Взломщики кодов». М.: Центрполиграф, 2000.

третий может перехватить передачу и выяснить факт передачи секретного сообщения, а возможно, и дешифровать его. Нужно сделать так, чтобы прочитать сообщение мог только Боб. В мире электронной связи отправка зашифрованного сообщения может вызвать сигнал тревоги со стороны специального программного обеспечения. Однако сообщение, скрытое средствами стеганографии, не вызовет никакой тревоги, поскольку кажется чем-то другим. Такое сообщение может быть размещено в открытом доступе. Способ скрытия при этом известен только Алисе и Бобу.

Стеганография используется уже давно. Книга германского аббата Иоганна Трисемуса (1462–1516) «The Steganographia» (Стеганография) была скорее оккультным, чем научным, трудом, соединяющим описание приемов стеганографии и текстов молитв. Первые буквы слов мистического произведения зашифровывали другие скрытые сообщения, а сама книга оставалась тайной целый век после написания.[1] Компьютеры создали беспрецедентные возможности для стеганографической коммуникации. Как простейший пример, возьмем обычный документ текстового процессора. Пусть это будет любовное письмо. Напечатайте его или просмотрите на экране – и не увидите ничего, кроме признания Алисы в своих чувствах к Бобу. Но в документе есть еще один, последний абзац, *в котором она изменила цвет шрифта на белый*. Текстовый процессор честно отображает белый текст на белом фоне. Если Боб знает секрет, он может прочесть последний абзац, например, изменив цвет фона секретного абзаца с помощью инструмента Highlighter Tool (примерно так и была восстановлена закрытая виртуальным маркером секретная информация о смерти Калипари).

Если бы кто-то еще догадался, что Алиса сделала что-то в этом роде, он мог бы проверить документ с помощью специальной программы. Но есть множество мест, в которых можно спрятать стеганографические сообщения, и множество способов скрытия. Поскольку латиница кодируется восьмибитными кодами, текст может быть скрыт внутри другого текста при условии наличия общих соглашений о кодировании. Какая буква скрыта в этом предложении?

```
Steganographic algorithms hide messages inside photos, text, and other data.
```

Ответ – «I» (ASCII-код 01001001). В первых восьми словах предложения начальные согласные кодируют 0, а гласные – 1 (рис. 3.15).

```
Steganographic algorithms hide messages inside photos, text, and other data.
0             1          0    0        1      0       0     1
```

Рис. 3.15. *Стеганографическое скрытие текста в тексте. В первых восьми словах предложения начальные согласные кодируют 0, а гласные – 1*

[1] Адам Маклин (Adam McLean) «The Steganographia of Johannes Trithemius» (Стеганография Иоганна Трисемуса), Magnum Opus Hermetic Sourceworks, Эдинбург, 1982 год.

Один весьма эффективный стеганографический метод заключается в незначительном изменении значений цветовых пикселов в изображении. Цвет определяется тремя составляющими – красной, зеленой и синей. В графическом файле каждому пикселу соответствует по три байта цветовых составляющих. Каждый байт интерпретируется как число от 0 до 255 и означает интенсивность соответствующего цвета. Изменение правого бита с 1 на 0 (например, изменение 00110011 на 00110010) уменьшает число на 1; в данном случае с 51 до 50. Изменение в результирующем цвете при этом незначительно, почти незаметно. Правые биты в изображениях могут нести много информации и не возбуждать при этом никаких подозрений. Получатель сообщения не визуализирует изображение, а обрабатывает биты и выделяет значащие нули и единицы.

Кто использует, если вообще использует, стеганографию сегодня? Трудно сказать. Газета *USA **Today*** сообщает, что террористы общались при помощи стеганографии в начале 2001 года.[1] Есть множество бесплатных программ для составления стеганографических сообщений. Стеганографические детекторы (правильнее называть их инструментами стеганализа) можно бесплатно скачать из Интернета (например, *www.cotse.com/tools/stega.htm* и *www.outguess.org/detection.php*), но их полезность весьма ограничена.

Стеганографические средства в наше время просты и недороги, а скрытые с их помощью сообщения практически необнаружимы. Иностранный шпион, который хочет за границей связаться с центром, может скрыть последовательность битов в файле формата MP3 или в порнографическом снимке. По миру перемещается такое количество музыки и порнографии, что обмен секретами с их помощью не вызовет никаких подозрений.

Пугающие секреты старых дисков

Возможно, к этому времени вас уже одолевает искушение удалить все с жесткого диска, а сам диск выбросить, чтобы больше не рисковать секретными файлами. Не спешите – даже удаленные файлы продолжают хранить старые секреты.

Несколько лет назад двое исследователей из Массачусетского технологического института купили – в основном, на аукционе eBay – 158 бывших в употреблении жестких дисков и восстановили данные с них. Большинство продавцов предприняло некоторые усилия, чтобы убрать

[1] Джек Келли (Jack Kelley) «Terror groups hide behind web encryption» (Группы террористов скрываются при помощи интернет-шифрования), *USA Today* от 5 февраля 2001. См. также Фархад Манджоо (Farhad Manjoo) «The case of the missing code» (Случай с пропавшим шифром), *Salon.com*, 17 июля 2002 года.

свои данные: они отправили файлы в «корзину». Некоторые зашли так далеко в удалении, что использовали команду FORMAT системы Microsoft Windows с ее предупреждением о том, что «все данные на диске будут уничтожены».

Только 12 из 158 дисков действительно были очищены от всех данных. Комбинируя несколько методов, исследователи восстановили пользовательские файлы с большинства оставшихся дисков. На 42 из них было найдено нечто, подозрительно напоминавшее номера кредитных карт. Один из дисков до продажи, по-видимому, обитал в банкомате в Иллинойсе и содержал 2868 номеров банковских счетов и сведений о балансе. Такие диски – просто сокровище для махинаторов. Однако большинство дисков были с домашних компьютеров и содержали весьма проникновенную личную информацию, например любовные письма, порнографию, жалобы на лечение рака у ребенка, выражения недовольства оплатой.[1] Многие диски хранили достаточно информации для установления личности бывшего владельца.

Большинство продавцов сделали то, что положено, – так или иначе удалили файлы. Возможно, они считали, что нельзя загрязнять окружающую среду токсичными материалами, выбрасывая старые компьютеры на помойку; но продавцы не знали, что выбросили свою персональную информацию в цифровую среду, поместив старые диски на аукцион eBay. Кто угодно со всего мира мог за несколько долларов приобрести диски вместе со всеми данными. Так что же здесь происходит, и что нам делать с этим?

Дисковое пространство поделено на блоки, которые можно сравнить со страницами книги: каждый блок имеет свой адрес, вроде номера страницы, и каждый может хранить несколько сотен байт данных, как строки текста на странице. Однако если размер файла превышает емкость блока, файл часто хранится не в соседних блоках. В каждом их таких блоков хранится не только фрагмент файла, но и адрес блока следующего фрагмента. Так что физически большой файл может быть разбросан по всему диску, в то время как логически файл представляет собой непрерывную последовательность ссылок предыдущих блоков на последующие. Это похоже на структуру журнала, где статьи не обязательно располагаются на соседних страницах. Часть статьи может заканчиваться фразой вроде «Продолжение на стр. 152», а часть со страницы 152 может указывать еще на какую-нибудь страницу и т. д.

Поскольку файлы на диске разбросаны случайным образом, есть *индекс*, хранящий записи об адресе начального блока каждого файла. Ин-

[1] Симсон Гарфинкель, Аби Шелат (Simson Garfinkel and Abhi Shelat) «Remembrance of Data Passed: A Study of Disk Sanitization Procedures» (В память об упущенных данных: уроки очистки диска), *IEEE Security and Privacy*, январь/февраль 2003, с. 17–27.

декс сам по себе является файлом, но его расположение на диске точно известно. Дисковый индекс – это что-то вроде указателя в книге, который всегда находится в конце. Найдя указатель, читатель может быстро найти номер страницы для каждого пункта и перелистать книгу до нужной страницы.

Cloud computing («облачные вычисления»)

Один из способов избежать проблем с удаленными файлами и дорогими офисными программами – хранить документы в другом месте! В технологии Cloud computing документы хранятся на дисках центрального сервис-провайдера и могут быть доступны через веб-броузер. Пример такого сервиса – Google Docs; но он не единственный, другие крупные компании тоже намерены выйти на рынок централизованных вычислений и хранения данных. Если вы доверяете хранение ваших документов корпорации Google, то сможете получить доступ к ним из любого узла Интернета и навсегда перестанете беспокоиться о том, что случайно удалите или потеряете файлы, ведь процедуры резервирования корпорации Google лучше тех, которые когда-либо могли быть у вас. Но есть и потенциальные проблемы. Юристы корпорации сами принимают решения о реакции на судебные запросы. Федеральные следователи вправе инспектировать биты, пересылаемые в пределах США и даже в другие страны.

Почему жесткие диски не организованы по образу книг, а документы не хранятся в последовательных блоках? Потому что диски обладают двумя важными отличиями от книг. Во-первых, диски динамичны. Информация на диске время от времени изменяется, добавляется и удаляется. Диск больше похож на металлический скоросшиватель, в который регулярно вставляют новые листы, чем на книгу. Во-вторых, жесткие диски – полностью перезаписываемые носители. Блок диска может содержать в один момент времени одну последовательность нолей и единиц, а в другой момент – другую последовательность, как результат операции записи. После операции записи уже невозможно сказать, какие биты находились там прежде. Это не то, что рисунок карандашом, который даже после стирания оставляет слабый след. Фактически само понятие «стирания» применительно к диску неуместно – происходит только замена одних битов другими.

В динамическом, не последовательном расположении файлов на дисках много плюсов. Например, если файл представляет собой большой текстовый документ, в середину которого пользователь добавляет несколько слов, то перезаписи подлежит только промежуточный блок логической цепочки. Если нужно добавить, допустим, пять блоков, то

они могут быть логически вписаны в цепочку без необходимости обновления всех последующих блоков. Аналогично, если часть текста удалена, то логическая цепочка исправляется так, чтобы «перепрыгнуть» через блоки, содержащие удаленный текст.

Блоки, не принадлежащие ни одному файлу, собираются в резерв, называемый *пулом*. Программное обеспечение компьютера ведет базу записей адресов блоков в пуле. Блок может быть зачислен в пул, если никогда не использовался или использовался, но был освобожден. Блок освобождается, когда файл, использующий его, удаляется или изменяется так, что данные блока удаляются. Когда появляется запрос на новый блок – к примеру, чтобы создать новый файл или дополнить имеющийся, – из пула выбирается очередная запись с адресом свободного блока.

Что происходит с данными при удалении файла?

Когда блоки освобождаются и добавляются в пул, их содержимое не перезаписывается. Когда блок выбрается из пула и становится частью другого файла, содержимое блока заполняется данными файла, а прежние данные теряются. Но до этого содержимое блока не изменяется. Целые файлы при удалении могут оставаться нетронутыми, за исключением того, что их становится довольно трудно отыскать. Просмотр индекса не даст ничего, потому что при удалении файла запись о нем стирается из индекса. Само же содержимое файла все еще находится где-то на диске. Информация в книге не уничтожается при вырывании страниц указателя. Чтобы найти нужный текст без указателя, вам придется пролистать какое-то количество страниц – это нудно и отнимает время, но информация найдется.

Примерно это и проделали исследователи с купленными дисками – читали данные с блоков, один за другим, в поисках определенных последовательностей битов. Ряд из 16 ASCII-кодов, представляющих десятичные числа, к примеру, подозрительно похож на номер кредитной карты. Даже если невозможно восстановить весь файл, часть блоков которого перезаписана, можно выявить короткие строки важных данных, таких как номера счетов.

Конечно, есть простой способ предотвратить сохранение важных данных в освобожденных блоках. Можно перепрограммировать компьютер так, чтобы освобожденные блоки не только помещались в пул, но и перезаписывались последовательностью нолей. Исторически производители компьютеров и программного обеспечения считали, что недостатки обнуления блоков превышают преимущества. Общество только недавно начало считать утечку данных важной проблемой – времена меняются. Затраты на регулярное обнуление блоков могут быть весьма значительными. Операция обнуления занимает время, и если бы функция обнуления была включена в системное программное обеспечение, то разработчики получали бы множество жалоб от

пользователей на низкую производительность компьютеров. При достаточно умелом программировании процесс обнуления можно сделать почти незаметным, но ни корпорация Microsoft, ни корпорация Apple не сочли нужным потратиться на это.

Что, если вы удалили файл и хотите его восстановить? К счастью, многие из нас обычно удаляют файлы перетаскиванием в «Корзину», удаляемые таким образом файлы не помещаются в пул: их можно вернуть, перетащив обратно из «Корзины». Файлы будут окончательно удалены из индекса при выполнении команды «Очистить корзину», но блоки при этом не обнуляются.

Слово закону

Нарастает беспокойство по поводу утечки данных, восстанавливаемых с дисков. Федеральная торговая комиссия (Federal Trade Commission, FTC) требует «разрушения или стирания данных с электронных носителей, содержащих информацию о потребителях, до степени, исключающей чтение или реконструкцию информации».[1] Подобное требование содержится и в законодательстве штата Массачусетс о нарушениях безопасности.[2]

Как насчет команды FORMAT операционной системы Windows (рис. 3.16)? Выполнение команды занимает примерно 20 минут. Видимо, в соответствии с предупреждающим сообщением действительно удаляются все биты данных.

На самом деле происходит нечто иное. Команда просто просматривает диск в поисках сбойных блоков. Физические повреждения на магнитной поверхности диска могут сделать отдельные блоки неработоспособными, даже если механика диска в это время работает исправно и остальная поверхность пригодна для хранения данных. Команда FORMAT выполняет чтение каждого блока, чтобы выявить и пометить сбойные блоки. Чтение всех блоков диска – дело долгое, однако, перезапись всех блоков происходит примерно вдвое дольше. Команда FORMAT обнаруживает сбойные блоки и повторно формирует индекс, но оставляет данные в большинстве блоков нетронутыми, так что их может восстановить ученый-исследователь – или просто продвинутый пользователь.

---

[1] Федеральная торговая комиссия, Кодекс административного законодательства США, том 16, часть 682 «Удаление информации о потребителях».

[2] Законодательство штата Массачусетс, часть 82 собрания 2007 года, «Акт о бездействии систем безопасности и уведомлении о потере контроля над данными», глава 93I.

```
Command Prompt - format c:
C:\>format c:
The type of the file system is NTFS.

WARNING, ALL DATA ON NON-REMOVABLE DISK
DRIVE C: WILL BE LOST!
Proceed with Format (Y/N)?
```

Рис. 3.16. *Вывод предупреждения команды* ***FORMAT операционной системы*** *Windows.* ***Предупреждение сообщает о потере всех данных – на самом деле*** *большая часть «удаленных» данных может быть восстановлена*

И как будто проблем с дисками было недостаточно, та же беда настигла владельцев сотовых телефонов. Когда люди избавляются от телефонов, то часто забывают очистить их память от журналов звонков и сообщений электронной почты. Даже те владельцы, которые решились прочесть инструкцию к аппарату и выполнить все описанные комбинации, могут получить совсем не те результаты, на которые рассчитывали.

Исследователь купил на аукционе eBay 10 подержанных сотовых телефонов и обнаружил много интересного: номера банковских счетов и пароли, планы корпоративной стратегии и почтовую переписку женщины и ее женатого любовника, чья супруга, кажется, начала что-то подозревать.[1] Информацию удалось восстановить даже с тех телефонов, память которых была очищена в соответствии с инструкциями компании-изготовителя.

Программы для необратимой очистки диска

Если вы действительно хотите полностью очистить свой диск на компьютере Macintosh, воспользуйтесь командой Secure empty trash. На компьютере с операционной системой Windows вы можете применить бесплатную программу DBAN, которая заполнит ваш диск битовыми нолями. Программа DBAN доступна на сайте *dban.sourceforge.net* (на сайте *sourceforge.net* много другого бесплатного программного обеспечения). Используйте подобные средства, только если вы абсолютно уверены в необходимости удаления всех данных!

В глобальном масштабе биты имеют сильное стремление к выживанию. И в большинстве случаев это то, чего мы хотим. Если компьютер

[1] Ларри Магид (Larry Magid) «Betrayed by a cell phone» (Предательство сотового телефона), *CBS News*, 30 августа 2006 года, *www.cbsnews.com/stories/2006/08/30/tech/main1949206.shtml*.

ломается, потерю легче перенести, зная, что корпорация Google хранит копии наших данных. Когда ломается сотовый телефон, какое это счастье – получить список контактов от оператора. В выживании битов есть и плюсы, и минусы.

Физическое разрушение как метод удаления данных работает всегда. Кто-то использует молоток, кто-то топор. Но вообще-то, такой метод не совсем удовлетворяет действующим требованиям к безопасной утилизации токсических материалов.

Можно ли стирать данные необратимо?

Время от времени появляются слухи о том, как инженеры, вооруженные высокочувствительной аппаратурой, могут найти разницу между нулем, записанным поверх нуля, и нулем, записанным поверх единицы. В теории, пространственно операция выполняется не очень точно – у бита есть своя площадь. При перезаписи границы битов могут не совпадать, давая возможность «рассмотреть» уголок перезаписанного бита. Если такие микроскопические несовпадения действительно могут быть обнаружены, то появляется возможность восстановления информации даже с *обнуленного* блока.

Для сохранения данных делайте копии

Если ваш компьютер когда-либо был подключен к вычислительной сети, то удаление данных с компьютера не затронет копии, хранящиеся на других узлах. Электронная почта пересылается к вам и от вас – другие могут хранить вашу почту и передавать ее еще кому-то. Если вы используете почтовый сервис Gmail, корпорация Google может хранить копии ваших сообщений, даже если вы их удалите. Если вы сделали заказ онлайн, то уничтожение соответствующих сведений на вашем компьютере не затронет записи в базе данных продавца.

Однако достоверных свидетельств существования подобных технологий нет, а с ростом плотности записи на жесткие диски вероятность возможного восстановления данных подобным образом уменьшается. С другой стороны, не исключено, что подобные технологии применяются в лабораториях спецслужб, а они вряд ли обнародуют свои достижения! В итоге можно сказать, что если восстановление перезаписанных данных путем сравнения микроскопических участков магнитной поверхности возможно, то доступно лишь горстке организаций, а сам способ настолько дорог, что восстанавливаемые данные должны иметь исключительную ценность.

Сколько в действительности «живут» данные?

Цифровая информация кажется вечной, и ее жизнь продляется копированием, что зачастую очень мешает хранению секретов, однако иногда возникает и прямо противоположное явление. Электронные записи могут вдруг стать недоступными, несмотря на все усилия увековечить ценные данные.

На рис. 3.17 показана средневековая геополитическая и демографическая база данных – Кадастровая книга Англии, опись английских земель, составленная в 1086 году по приказу Вильгельма Завоевателя. Книга является национальным достоянием Великобритании и хранится в государственном архиве во вполне читабельном состоянии.

Рис. 3.17. *Кадастровая книга Англии 1086 года*

Британский национальный архив

В 1986 году в честь девятисотой годовщины Кадастровой книги вещательная корпорация BBC выпустила в свет современную версию книги с фотографиями, текстами и картами. Цифровая книга была выпущена не на бумаге или пергаменте, а на 12-дюймовых видеодисках, которые могли быть прочитаны только на специальном компьютерном устройстве (рис. 3.18). Целью выпуска было сохранить сведения по истории и географии Англии XI века и сделать их общедоступными для школ и библиотек.

Уже в 2001 году современный вариант Кадастровой книги оказался нечитаемым. Компьютеры и необходимые устройства чтения дисков устарели и больше не выпускались. За 15 лет оказалась потеряна даже информация о форматах хранения данных книги. Иронизируя над грандиозными амбициями разработчиков, одна британская газета заметила: «Цифровая Кадастровая книга просуществовала не тысячу лет, а всего пятнадцать».[1]

[1] Робин МакКай и Ванесса Торп (Robin McKie, Vanessa Thorpe), *Guardian Unlimited* от 3 марта 2002 года. Веб-сайт проекта BBC оцифровки Кадастровой книги: *www.atsf.co.uk/dottext/domesday.html*.

Рис. 3.18. *Персональный компьютер середины 1980-х, оснащенный приводом для чтения 12-дюймовых видеодисков, содержащих цифровую Кадастровую книгу*

*Статья «**Domesday Redux**», **интернет-журнал «Ariadne», выпуск 36***

Рис. 3.19. *Усилия по восстановлению структуры форматов данных цифровой Кадастровой книги (после 2000 года)*

Можно прочитать листы бумаги и папируса, которые на тысячи лет старше оригинала Кадастровой книги. Электронные записи стали нечитаемыми за несколько лет. Сможет ли то огромное количество информации, что накоплено в наши дни на компьютерных носителях, быть прочитано через сто или тысячу лет в будущем? Или переход от бумаги к дискам приведет к потере истории?

У истории с цифровой Кадастровой книгой счастливый конец. Данные с дисков были восстановлены, хотя и с трудом, благодаря объединенным усилиям множества инженеров. Восстановление структуры форматов данных потребовало немало умственных усилий при разборе компьютерных кодов (рис. 3.19) и глубокого изучения литературы по форматам тех лет. Программисты смогли ясно представить, как разработчики 1980-х решали проблемы представления данных 15 лет назад. В мире компьютерных наук быть экспертом и идти в ногу со временем очень трудно.

Восстановленная современная цифровая версия Кадастровой книги теперь доступна всем желающим через Интернет. На веб-сайт были выложены даже оригинальные файлы данных.[1]

Сохранение «старой Паутины»

Программное обеспечение сайта Internet Archive (*www.archive.org*) периодически создает «снимки» общедоступных веб-сайтов и сохраняет в своем архиве. Любой пользователь Интернета может получить копию веб-страницы, когда-то существовавшей в прошлом, даже если на оригинальном сайте этой страницы нет или она была изменена. Установив в веб-броузере кнопку Wayback (доступна на сайте Internet Archive), вы можете увидеть, как та или иная страница выглядела в прошлом: просто загрузите страницу, нажмите кнопку Wayback, и вы получите список ссылок на архивные копии.

Здесь есть важная мораль для офисных и библиотечных сотрудников. Невозможно быть уверенным в том, что электронные архивы и диски, создаваемые в настоящее время, смогут быть прочтены спустя хотя бы 10 лет. Будут ли цифровые архивы (хотя бы та стопка дисков под кроватью, с некоторых пор заменяющая вам бабушкин фотоальбом) так же долговечны, как оригинальная Кадастровая книга? Предпринимаются чрезвычайные усилия по архивированию Всемирной паутины путем периодического создания копии всех общедоступных веб-страниц. Увенчается ли эта попытка успехом и будут ли архивные диски

[1] *www.domesdaybook.co.uk/index.html*

своевременно заменяться, чтобы информация сохранилась для нас навсегда?

Или же будет мудрее поступить «старым дедовским способом»: записать или напечатать все, что заслуживает длительного хранения (электронные журналы, например), так что документы будут храниться в единственной форме, доступной в любую эпоху?

Цифровая революция снабдила обычных людей мощными средствами документирования мыслей. Технологический прорыв сократил количество промежуточных звеньев, необходимых для создания офисных меморандумов и книг. Прибавилось и возможностей управления содержимым документов. Власть, которой обладали над документами владельцы письменных или напечатанных экземпляров, переместилась в руки составителей электронного содержания. Производство информации стало более демократичным, хотя результаты бывают разные, о чем красноречиво свидетельствуют описанные в этой главе казусы.

Перейдем ко второй половине рассказа: как мы получаем информацию, которую создают другие. Когда власть над документами была более централизованной, она принадлежала тем, кто имел возможность печатать книги, у кого были ключи от архивов или собрания документов и публикаций. Собрания документов могли быть как местами информационного «глушения», так и инструментами публичного образования. Библиотеки, к примеру, всегда были памятниками имперской мощи. Университетские библиотеки долго являлись центральными учреждениями высшего образования, а местные общественные библиотеки были основой демократизации для культурных наций.

Если все это – только биты и каждый может иметь столько битов, сколько захочет, то проблема может заключаться не в отсутствии информации, а в ее поиске. Даже зная, что факт есть у вас на компьютере, под рукой, не так-то легко отыскать нужные биты среди миллиардов прочих. Что толку в стоге сена, если в нем невозможно отыскать драгоценную иголку! В следующей главе мы зададимся вопросом: кому принадлежит реальная власть в новом мире, где доступ к информации означает не только обладание ей, но и возможность быстро найти нужные данные?

Глава 4 | Иголки в стоге сена

Корпорация Google и другие посредники на рынке битов

Найдены спустя семьдесят лет

Розалии Полоцкой было всего десять лет, когда она простилась со своими двоюродными сестрами Софией и Осси на московском вокзале. В 1937 году две сестры бежали от сталинских репрессий, чтобы начать новую жизнь. Семья Розалии осталась в Советском Союзе. Розалия выросла в Москве, изучила французский, вышла замуж за Наримана Берковича, посвятила себя семье. В 1990 году Розалия эмигрировала в США и поселилась рядом с сыном Сашей в штате Массачусетс.

Розалия, Нариман и Саша никогда не переставали интересоваться судьбой Софии и Осси. «Железный занавес» почти полностью перекрыл каналы коммуникаций между еврейскими семьями. К тому времени как Розалия отправилась в США, прошло уже столько лет, что надежд на воссоединение почти не осталось, да и вряд ли сестры были еще живы. По настойчивым просьбам деда Саша искал зацепки в эмигрантских записях Эллис-Айленда и Международного Красного Креста, но ничего не нашел. Возможно, пересекая охваченную войной Европу, маленькие девочки так никогда и не добрались до США.

Но однажды Сашин двоюродный брат, набрав фамилию Полоцкий (Polotsky) в строке поиска Google, обнаружил одну зацепку. В ссылке на генеалогический веб-сайт упоминалась фамилия Минакер (Minacker). Это была фамилия отца Софии и Осси. Вскоре Розалия, София и Осси смогли воссоединиться во Флориде, спустя 70 лет. «Все время, пока он был жив, он просил меня сделать все возможное, чтобы найти их, – говорил Саша, вспоминая просьбу своего деда. – Это просто чудо».[1]

---

[1] Ева Вольховер (Eva Wolchover) «Web reconnects cousins cut off by Iron Curtain» (Всемирная паутина соединяет двоюродных сестер, разделенных «железным занавесом»), *Boston Herald* от 18 декабря 2007 года; «Web post reunites cousins after 70 years» (Активный поиск в Интернете помог кузинам встретиться через 70 лет), *Associated Press Online* от 19 декабря 2007 года; электронные письма от Саши Берковича.

Цифровой взрыв выбросил в мир огромное количество информации, Интернет рассеял эти данные по всему миру, а Всемирная паутина сделала информацию доступной миллионам обычных людей. Но нельзя получить доступ к информации, даже не зная, где она находится. Колоссальные массивы цифровых данных все равно что не существуют, если на них невозможно выйти. Большинство пользователей находит нужное в Интернете с помощью поисковых систем. Поисковые системы – это поразительные, преображающие цифровой мир технологии, которые воплощают мечты и упорядочивают человеческое знание. Инструменты поиска, помогающие нам находить иголки в цифровых стогах, – как бинокль, через который можно обозревать цифровой ландшафт. Правительства и корпорации используют инструменты поиска для формирования нашего видения реальности.

Библиотека и базар

На заре своего существования Всемирная паутина была библиотекой. Информацию поставляли в основном корпорации и университеты, у которых была возможность создавать веб-страницы. Потребители информации – в основном другие компании и научные исследователи – получали сведения об информационных ресурсах и скачивали их. Сведения об источнике информации заключались в адресе, таком как URL (Uniform Resource Locator, универсальный локатор ресурса), например *mit.edu* (адрес URL Массачусетского технологического института). Обычные пользователи не имели доступа к пока-еще-не-всемирной паутине. Вместо нее пользователи получали доступ к онлайн-службам, например CompuServe, и их базам данных с различной информацией.

Web 1.0 против Web 2.0

Сегодня более интерактивные и зависящие от поведения пользователя сайты принято называть Web 2.0. Старые, более статичные сайты называют Web 1.0. Эти обозначения похожи на нумерацию версий программного обеспечения, но выражение «Web 2.0» обозначает нечто принципиально более тонкое и сложное. Сайты типа Web 2.0, например социальная сеть Facebook или сетевая энциклопедия Википедия, воплощают то, что экономисты называют «сетевым эффектом». Поскольку пользователи размещают свою информацию, одновременно получая доступ к информации, размещенной другими пользователями, ценность сайтов нового типа возрастает с ростом числа пользователей. Более подробное описание явления Web 2.0 на английском языке можно найти по адресу *http://www.oreillynet.com/lpt/a/6228*.

Когда Всемирная паутина стала коммерческим образованием, появились каталоги ресурсов, в том числе печатные «Желтые страницы». Такие каталоги содержат списки ресурсов, где можно заказать различные продукты или услуги. Хотите купить автомобиль – смотрите один раздел, ищете работу – другой. Каталоги заменили категории, которые онлайн-службы AOL и CompuServe предоставляли клиентам в те времена, когда прямого подключения к Интернету фактически не было. Каталоги редактировались людьми, со всеми вытекающими последствиями.

Состояние Всемирной паутины круто изменилось в середине 1990-х. Во-первых, она перестала быть пассивным информационным ресурсом. Блоги, Википедия и Facebook – это пополняемые структуры данных, где полезность информации определяется участием пользователей. Веб-сайты стоят недорого, и их легко создавать. Собственный сайт может завести и рядовой пользователь, и самая мелкая организация. В результате содержимое и структура связей в Интернете все время меняются.

Во-вторых, Всемирная паутина стала такой объемной и беспорядочной, что разделить все имеющиеся ресурсы на четкие категории просто невозможно. Веб-страницы не желают укладываться в понятную структуру или схему. Не существует никакого генерального плана – огромное количество новых веб-страниц ежедневно добавляется безо всякого намека на порядок. Глядя на URL веб-страницы, вы, скорее всего, не сможете определить, что она содержит.

Даже иерархическая организация не поможет найти нужную информацию, если вы сами не очень-то представляете, что именно ищете. Как правило, люди обращаются в Интернет не за определенной страницей, а за определенной информацией, и где она находится – не особенно важно. Если вы не знаете, в какой категории искать, структура вам не поможет. Возьмем, к примеру, такой строго структурированный источник знаний, как энциклопедия. В ней есть раздел «Человек» и раздел «Луна». Но если вы ищете детский стишок о лунном человечке, ни один из этих разделов не поможет вам выяснить, чем этот человечек у себя на Луне занимается. Но введя оба слова в строке запроса поисковой системы, вы, возможно, получите ответ в мгновение ока.

Функция поиска, причем не только по всему Интернету, – фактически обязательный сервис. На сайте торговой сети Wal-Mart товары разбиты по категориям. Щелкнув ссылку на одну из категорий, вы перейдете в новый раздел со списком подкатегорий товаров и так далее. Но в верхней части окна есть еще и инструмент поиска. Введите в строке поиска название нужного товара – и перейдете на страницу с его описанием (но только в пределах сайта сети Wal-Mart). Подобные локальные поисковые системы помогают обмениваться фотографиями, читать газеты, заказывать книги в интернет-магазинах Amazon или Barnes & Noble или даже разыскивать старую почту на своем компьютере.

Поисковая система – это новая форма контроля с помощью информации.

Функции поиска позволяют найти нужную информацию в больших цифровых хранилищах. Но наличие функции поиска – это не только быстрая альтернатива просмотру библиотечного каталога. *Поисковая система – это новая форма контроля с помощью информации.*

Поисковые службы вроде Google исключительно демократичны – чтобы найти пропавших родственниц, Розалии и Саше Берковичам не пришлось прибегать к услугам специальных розыскных агентств. Но создатели поисковых систем не только предоставили всем и каждому широкие возможности для поиска. Принимая и используя поисковые системы, люди передают им право называть наиболее авторитетные источники информации, например энциклопедии или информационные издания органов власти. Чрезмерное доверие поисковым системам позволяет им ограничивать количество информации, получаемой пользователями. Поиск в системе Google по запросу «демократия» в Китае выдаст совсем не то, что поиск по тому же запросу в США. Поиск по запросу «пенсионный план» на сайте инвестиционной компании John Hancock не даст ссылку на пенсионный план компании Fidelity.

Для пользователя сила поисковых систем заключается в их способности находить нужную информацию. Для владельца поискового сервиса сила в возможности выбирать, что показывать пользователям в ответ на их запросы. У поисковых систем есть и другое свойство – чем больше вы их используете, тем больше о вас известно. В своем ежегодном отчете «Zeitgeist» корпорация Google показывает статистику текущих тенденций и интересов пользователей, публикуя наиболее частые вопросы. Было удивительно узнать, что большинство вопросов типа «Кто такой ...» за 2007 год заканчивается словом «Бог» (первое место); «Сатана» на десятом месте, причем его опередил музыкант Бакетхед (шестое место).[1] Такая же статистика может вестись и о каждом отдельном пользователе. Как уже обсуждалось в главе 2, подобную статистику (и предложение «наиболее интересующих» клиента книг на ее основе) ведет интернет-магазин Amazon для каждого, кто хоть раз воспользовался его услугами.

Несколько интересных результатов из отчета «Zeitgeist» поисковика Google за 2007 год: среди вопросов типа «Что такое ...?» на первом месте «любовь», на десятом – «подагра»; среди вопросов типа «Как ...?» на первом месте «целоваться», на десятом – «кататься на скейтборде».

[1] *www.google.com/intl/en/press/zeitgeist2007/mind.html.*

Бритни на базаре битов

Удовлетворение запросов большинства ведет к тирании большинства и пренебрежению интересами меньшинства. К примеру, авторы, выполняя запрос по слову «spears», получили три страницы ссылок на певицу Бритни Спирс и ее сестру и всего три исключения: компания по производству труб из ПВХ Spears Manufacturing, комедиант Арий Спирс и профессор Уильям М. Спирс из Университета Вайоминга. Забавно, что ссылка на веб-страницу профессора Спирса находилась дальше от начала списка, чем ссылка на сайт под названием «Руководство Бритни Спирс по физике полупроводников» («Britney Spears' Guide to Semiconductor Physics»), поддерживаемый несколькими бесшабашными физиками из Университета Эссекса в Великобритании. У последнего сайта было характерное название – *britneyspears.ac*, где «.ac» означает не «academic» (академический), а «Ascension Island» (остров Вознесения), для которого стоимость доменного имени второго уровня составляет всего несколько пенсов.

Всемирную паутину уже нельзя сравнивать с библиотекой, скорее это базар, хаотическое движение миллиардов идей и фактов, порожденное цифровым взрывом. Потребители и поставщики информации постоянно ищут друг друга, ежедневно меняясь ролями. На этом призрачном базаре битов, с его носящимися слухами и бегающими туда-сюда разносчиками, поисковые системы выступают посредниками. Их работа заключается не в выяснении истины и не в экспертной оценке поставляемых материалов. Поисковые системы сводят нужных поставщиков с нужными потребителями информации. Успех или неудача битовых посредников зависит не от качества поставляемой ими информации (потому что они ее не поставляют вовсе), а от того, довольны ли встречей поставщик и потребитель. На рынке лучшие сделки часто заключает не самый высоколобый посредник. Чтобы оставаться в бизнесе, посредник должен только быть готовым в любое время предоставить клиентам то, что им нужно, и образовать наилучшие связи.

Поисковые системы не просто находят для нас ссылки. Они помогают нам открывать вещи, о которых мы даже не догадывались. Поиск в мире битов позволяет каждому, не вставая с кресла, почувствовать себя сыщиком, вытаскивающим с цифровой полки книгу за книгой, пока не найдется улика, и сопоставляющим фрагменты информации, повсюду оставленные цифровым нашествием.

До запретного плода – всего один щелчок

Шизофрения – опасное заболевание мозга, поразившее миллионы людей. Если вы хотите узнать больше о новейших способах лечения, то можете попробовать найти информацию на различных веб-сайтах.

Некоторые уже знают, где можно найти актуальную медицинскую информацию: у них в броузере есть закладка на надежный сайт, например, *WebMD.com* или *DrKoop.com*. Если же вы действуете, подобно нам, то воспользуетесь каким-либо поисковым сервисом, например *Google.com*, *Yahoo.com* или *Ask.com*. Вы введете в строке поиска несколько слов запроса и начнете исследовать ссылки. Конечно, не нужно слепо верить всему, что вы узнаете из случайных источников, или выполнять найденные инструкции, не посоветовавшись с врачом.

Введя в строке поиска сайта Google строку «schizophrenia drugs» (лекарства от шизофрении), авторы получили результаты, показанные на рис. 4.1. В верхней строке сообщается, что если нас не устраивает показанное, то к нашим услугам еще четверть миллиона ссылок. Там же присутствует время, затраченное на поиск, шесть сотых секунды (мы-то вообще не ощутили никакой задержки). Три «рекламных ссылки» справа означают, что кто-то заплатил компании Google за показ

Рис. 4.1. *Результаты, выданные поисковой системой Google по запросу «schizophrenia drugs»*

Google™ является зарегистрированной торговой маркой. Перепечатка с разрешения корпорации Google

ссылок «вне очереди». Слева расположен список простых ссылок, которые, по мнению алгоритма поиска, в первую очередь заинтересуют всех тех, кому нужны «лекарства от шизофрении», – это называется естественным результатом работы поисковой системы.

Быстрый взгляд на это окно порождает сразу несколько важных вопросов:

- Всемирная паутина колоссальна. Как поисковая система так быстро находит эти результаты? Находит ли она действительно нужные ссылки?
- На основе чего поисковый алгоритм решает, какой результат будет показан первым, а какой – 283 000-м?
- Даст ли другая поисковая система другой результат? Как правильно выбрать? Какой результат лучше? Какой достовернее?
- Рекламные ссылки лучше или хуже, чем естественные? Эта реклама действительно необходима?
- Что из всего этого находится под присмотром государства? Если телестанция продолжает передавать ложь под видом правды, государство придет и вмешается. Может ли государство повлиять на работу поисковых систем?

В свое время мы подробно ответим на эти вопросы, а пока продолжим наше медицинское «расследование».

Эти забавные имена

Слово Yahoo! является аббревиатурой фразы «Yet Another Hierarchical Officious Oracle» (еще один иерархичный услужливый советник), о чем можно узнать по адресу *docs.yahoo.com/info/misc/history.html*. Название Google происходит от слова «googol» («гугль»), обозначающего число, равное единице с сотней нолей. Основатели явно мыслят масштабно!

Пройдя по первой естественной ссылке, мы попали на веб-страницу специализированного шведского университета. Страница содержала некоторую информацию по лекарствам от шизофрении. Одно из них называлось «olanzapin (Zyprexa)». Название торговой марки пробудило некоторые ассоциации, так что мы вернулись к начальной странице поиска и запросили «Zyprexa».

Первая из естественных ссылок вела на сайт *www.zyprexa.com* с заголовком «The Official ZYPREXA Olanzapine Site» («Официальный сайт средства оланзапин фирмы ZYPREXA). На странице сообщалось, что сайт принадлежит производителю лекарственных средств Эли Лилли и К°. Было также много сведений о лекарстве, фотографии улыбающихся людей, очевидно, исцеленных пациентов, и слоганы типа

«Ваша надежда здесь» или «Откройте новые возможности». Следующие ссылки в результатах поиска вели на сайты с медицинской информацией *drugs.com*, *rxlist.com*, *webmd.com* и *askapatient.com*.

И сразу после них шла ссылка совершенно обратного направления: «ZyprexaKills wiki» («мини-справочник „Как Zyprexa убивает“»). Она вела на сайт, где сообщалось, что у лекарства есть весьма серьезные побочные эффекты, о чем производитель долгое время не упоминал. Единственная рекламная ссылка на странице результатов поиска называлась так: «Prescription Drug Lawsuit. Zyprexa-olanzapine-lawyer.com. Pancreatitis & diabetes caused by this drug? Get legal help today. («Судебные разбирательства по опасным рецептам. Сайт Zyprexa-olanzapine-lawyer.com. Прием лекарства вызвал панкреатит и диабет? Получите правовую помощь уже сегодня»). Ссылка вела на сайт, где правозащитник из Хьюстона предлагал представлять интересы посетителей против производителя лекарства (требовалось заполнить веб-форму).

Еще несколько щелчков мышью – и перед нами документ, озаглавленный «Оланзапин – изменение содержания глюкозы в крови» (рис. 4.2). Это был внутренний меморандум Эли Лилли и К°, не предназначенный для распространения за пределами компании и отмеченный как вещественное доказательство. Некоторые пациенты, получившие диабет при использовании лекарства, судились с производителем. Этот меморандум и другие документы были предоставлены адвокатам потерпевших в обычном процессуальном порядке. После серии не совсем законных действий адвокатов документы получил репортер *New York Times*.[1] Затем появилась статья о задержке производителем информации о побочных действиях оланзапина, а сами документы всплыли на множестве сайтов.

Представитель компании Эли Лилли и К° потребовал вернуть документы, уничтожить все копии и принудить веб-сайты убрать цифровые копии из открытого доступа. Началась правовая дуэль. 13 февраля 2007 года судья окружного суда Нью-Йорка Джек Б. Вайнштайн вынес решение. Распространение секретных документов признавалось незаконным и противоречащим более ранним постановлениям. Адвокаты и журналист совершили правонарушение против правовой системы, находясь в тайном сговоре с адвокатом из Аляски, который не имел права передавать кому-либо указанные документы. Адвокатам предписывалось вернуть документы без права сохранения каких-либо копий у себя или передачи копий кому-либо.

---

[1] Алекс Беренсон (Alex Berenson) «Lilly said to play down risk of top pill» (Лилли сообщает о снижении риска передозировки), *New York Times* от 17 декабря 2006 года; Алекс Беренсон «Drug files show maker promoted unapproved use» (Создатель шоу с лекарствами продвигает неодобренное использование), *New York Times* от 18 декабря 2006 года.

OLANZAPINE - BLOOD GLUCOSE CHANGES

SUMMARY

OLANZAPINE_AND GLYCEMIA

Zyprexa MDL 1596 Confidential-Subject to Protective Order
Zyprexa MDL Plaintiffs' Exhibit No.00916

Рис. 4.2. *Верхняя и нижняя строки документа означают подшивку судебного дела. Предполагалось хранить этот документ в тайне, но он появился в Интернете, так что любой, кто ищет по запросу «Zyprexa documents», легко найдет файл*

Источник: www.furiousseasons.com/zyprexa%20documents/ZY1%20%20%2000008758.pdf

Но, по мнению судьи Вайнштайна, решение не касалось веб-сайтов, поэтому в предписании не было приказа сайтам удалить цифровые копии документов. Производитель лекарств получил право вернуть бумажные копии, но вернуть биты было невозможно. Во время написания этой книги цифровые документы все еще были доступны, их можно было найти с помощью поисковой системы по запросу «zyprexa documents».

Мир сильно изменился с тех пор, когда судья мог спокойно приказать изъять *все* копии судебных материалов. Даже если бы существовали сотни копий, хранимых в секретерах и архивах, судья мог настаивать на возврате всех копий под угрозой судебного преследования. Но Всемирная паутина – это не архив или секретер. «Веб-сайты, – указал судья Вайнштайн, – это, главным образом, средства массового общения». Производитель оланзапина призывал запретить пяти сайтам публиковать эти материалы. Но миллионы других сайтов могли сделать это в будущем. «Бесполезно ограничивать свободу общения возможных распространителей путем запрета такого ничтожно малого числа сайтов» – заключил судья.[1]

Судья ясно понимал всю серьезность дела, решение по которому вынес. В сущности, попытка применить власть закона оказалась бы тщетной – нельзя запретить людям говорить то, что они хотят сказать, и узнавать то, что они считают важным выяснить. Даже если документы были выпущены из рук лишь на малое время, бессчетное количество копий могло успеть распространиться среди всех заинтересованных сторон.

[1] Суд Восточного округа Нью-Йорка, дело Zyprexa, 07-CV-0504, In re Injunction, I, IV.F, 13 февраля 2007 года.

Подыскивая аналогию, судья заметил, что даже Господь Бог потерпел неудачу в Его попытке запретить Адаму и Еве вкусить плод истины.

При поиске по запросу «zyprexa documents» появились две рекламные ссылки. Одна из них принадлежала еще одному адвокату, предлагающему представлять интересы пострадавших от приема оланзапина. Другая ссылка, с выделенным словом «документы», принадлежала самой поисковой системе: «Создавайте документы и работайте над ними в Интернете совместно с другими пользователями. Это абсолютно бесплатно. Узнайте больше. docs.google.com». Ироничное напоминание о том, что биты окружают нас, и что средства для их размножения тоже здесь, под рукой, доступные всем и каждому. Благодаря поисковым системам любой может найти интересущую его информацию – она вырвалась на информационные просторы.

Фактически, с созданием поисковых систем изменилась архитектура человеческого знания. За десять лет мы смогли освободиться от информационных пут, которые были с нами с начала письменной истории. Многие еще не осознали, что на самом деле случилось. Например, в феврале 2008 года суд Сан-Франциско вынес решение о закрытии сайта проекта Wikileaks, на котором публиковались подвергшиеся «утечке» конфиденциальные документы. Судья постановил удалить имя «Wikileaks» из баз данных серверов DNS, чтобы адресу *Wikileaks.org* больше не соответствовал IP-адрес. (В структуре Интернета серверы DNS отвечают за трансляцию адресов URL в IP-адреса, см. Приложение.) Общественность отреагировала на судебное решение созданием множества «зеркал» – копий исходного сайта, – которые можно было найти с помощью поисковых систем по запросу «Wikileaks».

Крушение иерархии

Долгое время человечество организовывало вещи, деля их на категории, подкатегории и так далее. Еще Аристотель пытался все классифицировать. Например, живых существ он делил на растения и животных. Животные разделялись на теплокровных и холоднокровных, теплокровные – на живородящих и яйцекладущих, к живородящим относились человек и другие млекопитающие, яйцекладущие делились на водоплавающих и воздухоплавающих и так далее. Губки, летучие мыши, киты представлялись Аристотелю зоологическими загадками. В начале эпохи Просвещения Линней предложил более удобную для науки классификацию живых существ, опирающуюся на степень их эволюционного развития и родства.

Следы нашей преданности иерархическим классификациям видны повсюду. Мы просто обожаем планы и схемы. Например, закон, охраняющий авторские права, обозначен в общей системе права как Книга 17, Секция 1201, Параграф (a), Часть (1), Подчасть (A). В Библиотеке Конгресса каждая книга относится к одной их 26 главных

категорий, обозначенных буквами латинского алфавита, подкатегории обозначаются аналогично, например категория B – философия, а BQ – буддизм.

Понимая категории, можно использовать классификацию для поиска нужных данных. При этом ищущий должен не только разбираться в системе классификации, но и определять необходимые признаки предмета поисков. К примеру, ища сведения о китах по классификации Аристотеля, требовалось бы *уже* знать, рыба кит или млекопитающее, чтобы попасть на нужную ветвь иерархического дерева. По мере того как все больше знаний классифицируется, дерево иерархии разрастается, создает новые ветви, которые, в свою очередь, пускают собственные отростки. Проблема классификации становится неконтролируемой, а получение данных – все более непростым, если вообще возможным.

Система веб-адресов тоже является иерархическим деревом. Адрес *www.physics.harvard.edu* указывает на веб-сервер физического факультета Гарвардского университета, где суффикс *.edu* означает «educational», то есть образовательный ресурс. Этот адрес вполне предсказуем, но с ростом Интернета система доменных имен становится все менее пригодной для поиска на ее основе. Нужно знать точный адрес.

В 1991 году, когда Интернет еще не был известен за пределами правительственных и образовательных учреждений, несколько университетских исследователей предложили проект программы Gopher. Эта программа создавала иерархический каталог веб-ресурсов, организуя файловые хранилища отдельных сайтов в одну большую карту-схему.

Название Gopher (суслик) было игрой слов: это была программа, которая позволяла «докопаться» («go for», произносится так же, как «gopher») до нужной информации в Интернете. Суслик также является талисманом университета Миннесоты, где была создана первая версия программы.

По нынешним меркам поиск с помощью сервиса Gopher был довольно утомительным; к тому же результат зависел от организаторских способностей администраторов отдельных сайтов. В 1994 году, как альтернатива, был создан интернет-каталог Yahoo!, редакторы которого разделяли продукты и услуги по категориям, давали рекомендации и старались сделать Интернет более доступным для непрофессионалов. Хотя уже давно главным сервисом Yahoo! остается окно приглашения поисковой системы, базовая функция каталога сохранилась до наших дней.

Практические ограничения иерархических организаций были предсказаны 60 лет назад. Во время Второй мировой войны президент США Франклин Рузвельт назначил Ванневара Буша из Массачусетского технологического института на должность директора Управления стратегических исследований и разработок (Office of Strategic Research and Development, OSRD). Управление координировало военные научные исследования. Это была тяжелая работа – 30 тысяч человек и сотни проектов из разных областей науки и техники. «Манхэттенский проект», завершившийся созданием атомной бомбы, был лишь одним из многих направлений.

Находясь на такой удобной точке обзора, Ванневар Буш сумел увидеть главную помеху дальнейшему научному прогрессу. Новая информация поступала быстрее, чем ее можно было использовать или хотя бы классифицировать. За десятилетия до того, как компьютеры стали распространенным явлением, исследователь изложил свои заключения в пророческой статье «As We May Think» (Как мы могли бы мыслить). Статья была опубликована в популярном (не техническом!) журнале *Atlantic Monthly*. Буш писал:

> Трудность, видимо состоит не в ошибочности публикаций, а в их количестве, далеко превосходящем наши возможности по практическому применению научных работ. Суммарный объем человеческого опыта возрос до невообразимых размеров, а средства, которые мы используем для того, чтобы пробраться по архипелагу информации к нужному островку, не намного быстрее приводят нас к цели, чем морские лоты времен парусных кораблей... Наша неспособность найти нужные данные в значительной степени связана с искусственностью существующих систем каталогизации.[1]

Рассвет цифровой эры тогда едва брезжил на горизонте. Но Ванневар Буш уже мечтал о машине, которую он назвал «memex» и которая расширила бы возможности человеческой памяти, сохраняя и восстанавливая всю необходимую информацию. Это было бы «расширенное внутреннее дополнение» к человеческой памяти, к которому можно было бы «обращаться с высочайшей скоростью и избирательностью».

Исследователь четко обозначил проблему, но современные ему технологии – микрофильмы и электронные лампы – не способствовали воплощению решения. Ванневар Буш понимал, что проблема поиска информации существенно замедлит научный прогресс, создание и сохранение новых знаний. Буша тревожило то, что цивилизация во время войны подвергалась серьезной опасности, но он призывал смотреть с оптимизмом на новые возможности, которые могли бы открыться при воплощении его идей. Человек «может пострадать в конфликте, если не научится использовать информацию во благо. В приспосабли-

[1] Ванневар Буш (Vannevar Bush) «As we may think» (Как мы могли бы мыслить), *Atlantic Monthly*, июль 1945 года.

вании научных знаний к удовлетворению потребностей и желаний людей информационный затор окажется своеобразной неудачной фазой, на которой прогресс завершится или не оставит надежд на результат».

Футуристический прецедент

В 1937 году фантаст Герберт Уэллс предвосхитил идею Ванневара Буша о машине «memex». Уэллс даже более подробно описал возможности каталогизации всего на свете и значение такого сверхкаталога для цивилизации:

> *Больше нет никаких практических препятствий для создания действенного каталога всех человеческих знаний, идей, достижений и появления таким образом всеобъемлющей планетарной памяти для всего человечества. И не просто каталога: прямое воспроизведение любой вещи может быть осуществлено в любой правильно подготовленной точке... Это факт исключительного значения. Он предвещает настоящее интеллектуальное равенство в нашей гонке. Вся память человечества в недалеком будущем может стать доступной каждому человеку... Это не отвлеченная мечта, не фантазия.*[1]

Возможности, казавшиеся фантастическими в то время, в наши дни распространены повсеместно. Цифровые вычислительные машины, емкие носители и высокоскоростные информационные сети породили необходимость в средствах поиска и извлечения информации и сами сделали создание таких средств возможным. Всемирная паутина реализовала идею машины «memex» Ванневара Буша, а поисковые системы позволяют быстро обращаться к электронной «памяти» Интернета.

Как это работает

Как могут поисковые системы Google и Yahoo! обработать вопрос, который им, возможно, никто раньше не задавал, и за долю секунды получить ответ от машин со всего света? На самом деле, поисковая система не опрашивает компьютеры по всему свету, чтобы ответить на ваш вопрос. С этой задачей нельзя справиться быстро – десятки секунд займет только пересылка битов во все концы. Вместо опроса всего Ин-

[1] Герберт Уэллс (H. G. Wells) «The idea of a permanent world encylopaedia» (План всемирной энциклопедии), *World Brain*, Мэтьен, 1938 год, с. 60–61. Статья доступна в Интернете: *sherlock.sims.berkeley.edu/wells/world_brain.html*.

тернета поисковая система использует *уже готовый* каталог, или индекс, и ищет ответ в нем, а затем пересылает вам ответ. Чтобы не обсуждать тонкости функционирования конкретной поисковой системы вроде Google или Yahoo!, представим себе гипотетическую поисковую систему с женским именем Джен. Джен выполняет набор процессов, обеспечивающий иллюзию мгновенной обработки запроса и выдачи множества более или менее верных ответов. Первые три процесса, или шага, не имеют отношения к вашему сеансу работы с Джен. Эти шаги непрерывно повторяются независимо от наличия или отсутствия в это время сеансов работы с пользователями. В компьютерной терминологии это называется *фоновым выполнением*.

1. **Сбор информации**. Джен исследует Интернет, регулярно просматривая множество веб-сайтов, чтобы узнать об их содержимом. Джен посещает существующие страницы повторно, чтобы узнать, не обновилось ли их содержимое и не появились ли ссылки на новые страницы.
2. **Сохранение копий**. Джен сохраняет копии посещенных страниц. На дисках компьютеров Джен хранится копия значительной части Всемирной паутины.
3. **Формирование индекса**. Джен конструирует колоссальную структуру данных, которая хранит, как минимум, список слов для каждой страницы.

Когда вы вводите запрос, Джен делает следующие 4 шага (уже на *переднем плане*):

4. **Разбор текста запроса**. В языке есть множество неоднозначностей. Запрос типа «red sox pitchers» («красный + носки + кувшины/бруски/подающие игроки»; как будет видно далее, запрос означает «подающие игроки бейсбольной команды Red Sox») может поставить в тупик, если вы не выросли на бейсбольном поле.
5. **Определение адекватности каждого из полученных результатов**. Содержит ли веб-страница нужную информацию?
6. **Определение приоритетности полученных результатов**. Какой из них является лучшим?
7. **Представление результатов**. Результат обработки запроса должен быть не просто «хорошим»; ответ также должен быть представлен в удобной форме и по возможности выполнить некоторые собственные задачи Джен, например показать рекламные ссылки.

Каждый из этих семи шагов содержит технические задачи, которые любят решать программисты. И спонсоры «проекта Джен» надеются, что инженеры предложат им лучшие решения, чем у конкурентов.

Мы подробно опишем каждый шаг, так как очень важно составить представление о происходящем, не углубляясь в технические особенности. Для каждого шага будут показаны возможности Джен по об-

работке информации – возможно, неожиданные способы сбора и преобразования данных, – которые затем формируют ваш взгляд на мир сквозь призму результатов поиска.

Фоновое выполнение подобно изготовлению декораций и проведению репетиций в театре. Без предварительной работы постановка не состоится; кроме того, нельзя выполнять эти действия при зрителях. Также у предварительных действий нет жесткого расписания.

Шаг 1: сбор информации

Поисковые системы не индексируют абсолютно все. Системы, так сказать, общего назначения – Google, Yahoo! и Ask – обрабатывают информацию подряд. Другие системы могут индексировать только сайты, относящиеся к определенной сфере. Поисковая система Medline выполняет поиск по медицинской литературе, ArtCylopedia индексирует 2600 сайтов, посвященных искусству, FindLaw LawCrawler обрабатывает только сайты из области права. Прежде всего, для любого поисковика есть сайты индексированные и неиндексированные, в зависимости от того, были или нет они посещены на первом шаге. Существуют некие критерии того, стоит ли вообще индексировать содержимое сайта. Итак, если сайт не был обработан поисковой системой на первом шаге, ссылка на сайт никогда не появится на седьмом.

Обращаясь к Ассоциации национальных рекламодателей (Association of National Advertisers) в октябре 2005 года[1], генеральный директор корпорации Google Эрик Шмидт заметил, что из 5000 терабайтов информации во всем мире проиндексировано только 170 (*терабайт* – около триллиона байт). Это количество составляет всего около 3%, так что остальные 97% информации остаются вне каталогов.[2] По другим оценкам, индексация охватывает всего 0,02% документов и баз данных, доступных во Всемирной паутине. При том что Всемирная паутина составляет только часть Интернета, Джен еще должна выбрать, какие сайты просматривать и как часто. Джен решает, что важно, а что – нет, ограничивая таким образом широту обзора пользователей.

Частота посещения веб-сайтов системой Джен – одна из ее тщательно охраняемых коммерческих тайн. Возможно, она ежедневно посещает новостные сайты, такие как *CNN.com* (служба новостей Си-Эн-Эн), так что если вы вечером поинтересуетесь утренними новостями, то Джен предоставит вам их ссылки. Скорее всего, у Джен есть особый список сайтов, которые часто изменяются и представляют общественный интерес, например *whitehouse.gov* (администрация президента США).

---

[1] Эрик Шмидт (Eric Schmidt) «Technology is Making Marketing Accountable» (Технологии позволяют вести маркетинговые расчеты), выступление перед Ассоциацией национальных рекламодателей 8 октября 2005 года, *www.google.com/press/podium/ana.html*.

[2] *www.ericdigests.org/2002-2/hidden.htm*

С другой стороны, Джен может обнаружить в своих поисках, что некоторые сайты вообще не изменяются, к примеру, онлайн-версия старой газетной статьи. Посетив такую страницу несколько раз, Джен решает зайти снова попозже, скажем через годик (на всякий случай). Третья разновидность страниц может просуществовать недостаточно долго, чтобы успеть попасть в индекс. Если разместить объявление о продаже на виртуальной доске сервиса *Craigslist.com*, оно станет видимым для других через пару минут. Если сделка будет быстро заключена, то объявление исчезнет и Джен его никогда не увидит. Даже если объявление продержится несколько дней, большинство поисковых систем могут его не проиндексировать.

Джен разумно решает вопрос частоты посещения веб-страниц, однако эта разумность подчиняется некоторым правилам и может *контролироваться*. Чем более важным считает Джен ваш сайт, тем меньше времени пройдет от внесения изменений в его содержимое до их появления в ответах Джен на запросы ее пользователей.

Джен путешествует по Интернету и собирает информацию путем перехода по ссылкам. Программа, исследующая Всемирную паутину, называется «пауком» (типичная шутка технарей). «Ползание по паутине» занимает дни или даже недели, так что Джен не может немедленно узнать о том, что какая-то страница или целый сайт больше не существует, и удалить неверные ссылки. В промежутках между посещениями Джен продолжает хранить в своем индексе недействительные ссылки и может выдавать их в ответ на запросы пользователей. Щелкните по такой ссылке, и появится сообщение вроде «Page not found» (Страница не найдена) или «Can't find the server» (Невозможно найти сервер).

Поскольку Всемирная паутина довольно хаотична, не существует абсолютно правильного и неизменного маршрута посещений страниц. Страница А может указывать на страницу Б, а страница Б может содержать ссылку обратно на страницу А, так что паук должен следить за тем, чтобы не зациклиться. Джен должна так организовать маршрут следования паука, чтобы посетить возможно большее количество страниц, избегая ненужных повторных посещений.

Веб-сайт может указать паукам, что не следует посещать страницы слишком часто или что не следует их индексировать. Разработчик сайта просто помещает необходимые директивы в файл *robots.txt*, и, в общем случае, пауки следуют прописанным указаниям. Конечно же, страницы, требующие авторизации, вообще не могут быть просмотрены. Итак, результаты поиска, выдаваемые на седьмом шаге, могут изменяться как в зависимости от сайтов, не желающих, чтобы Джен о них узнала, так и в зависимости от мнения Джен о том, кому и что следует знать. К примеру, Саше Берковичу сильно повезло, что генеалогическое дерево семьи Полоцких располагалось в общедоступном

разделе сайта *genealogy.com* – иначе паук системы Google не смог бы проиндексировать данные с дерева.

Наконец, индексация требует серьезных затрат. Посещения Джен являются обычными запросами к сайтам и требуют пересылки страниц. Действия пауков порождают дополнительный обмен информацией, увеличивая нагрузку на веб-сервер. Другими словами, фоновая часть работы поисковых систем создает нежелательные эффекты в работе всего Интернета. Работа пауков поглощает часть пропускной способности каналов связи и может «подвесить» сервер, который будет отправлять страницы паукам, заставляя ждать обычных пользователей. Коммерческие поисковые системы стараются нормировать работу пауков так, чтобы не перегружать посещаемые серверы.

Как паук исследует Паутину

Поисковая система собирает информацию путем «путешествия» по Всемирной паутине. Например, посетив главную страницу американского издателя этой книги *www.pearson.com*, паук получает от сервера текст, фрагмент которого приведен ниже.

```
<div id="subsidiary">
<h2 class="hide">Subsidiary sites links</h2>
<label for="subsidiarySites" class=«hide»>Available
sites</label>
<select name="subsidiarySites" id="subsidiarySites" size="1">
<option value="">Browse sites</option>
<optgroup label=«FT Group»>
<option value="http://www.ftchinese.com/sc/index.jsp">
Chinese.FT.com</option>
<option value="http://ftd.de/">FT Deutschland</option>
```

Эта компьютерная программа написана на специальном языке, который называется HTML (HyperText Markup Language – язык разметки гипертекста). Ваш веб-броузер формирует внешний вид веб-страницы путем выполнения этой программы. Но паук получает текст программы не для отображения страницы, а для индексирования ее содержимого. После обработки текста броузером на экране появится, к примеру, строка «FT Deutschland». Ее текст будет занесен в индекс. Паук распознает в тексте ссылки на другие страницы, получает их содержимое, индексирует его и так далее.

Паук, или веб-червь (web crawler), является разновидностью бота (bot). Бот (как в слове «робот») – это программа, которая циклически выполняет некоторую повторяющуюся операцию, обычно по сбору информации.

Шаг 2: сохранение копий

Джен сохраняет копии каждой страницы, посещаемой пауком. В отличие от броузера, формирующего внешний вид веб-страницы, Джен индексирует страницу. Если нужно, Джен может сохранить копию страницы на жестком диске своего компьютера – это называется *кэшированием* (от франц. cache – скрытый). Обычно Джен ничего не делает с копией, которая может очень скоро устареть. Однако кэширование позволяет Джен получить копию уже не существующей страницы или сделать доступной ее прежнюю версию. Это ответ Джен на слишком короткое время существования страниц, которые система не успела проиндексировать. Кэшированная копия позволяет Джен делать предположения об обычном содержании таких страниц.

Кэширование – еще один камешек в огород тех, кто любит сравнивать Всемирную паутину с библиотекой, потому что удаление информации с сайта не всегда означает прекращение доступа к ней. Авторы информации не могут убрать ее навсегда, после того как однажды опубликовали. К примеру, после 11 сентября 2001 года с сайтов было убрано много информации.[1] За одни сутки исчезли отчеты по правительственной уязвимости, важные данные по безопасности и даже отчет по химическому терроризму Центра контроля и профилактики заболеваний (Center for Disease Control and Prevention), вскрывший серьезные проступки промышленности. Но эти страницы были кэшированы поисковой системой Google и другими, так что продолжали оставаться доступными.[2]

Страницы с опасной информацией не только сохранились, но и оказались доступными всем пользователям Интернета. Каждый раз при использовании поисковой системы вы можете получить доступ к странице, сохраненной в кэше, а также ссылку на первоисточник, вне зависимости от того, существует он до сих пор или нет.Щелчок на ссылке кэшированной страницы выдаст вам нечто похожее на исходный ресурс. Пример кэшированной веб-страницы показан на рис. 4.3.

Вот реальный пример. Было опубликовано заявление ректора Лоуренса Саммерса от 17 января 2005 года после обнародования его слов о женщинах в науке. Как сообщалось в номере журнала *Harvard Magazine* за март-апрель 2005 года, заявление начиналось так: «Мои замечания были искажены таким образом, что из них следовало, будто я считаю, что женщины не способны достигнуть высокого уровня в математике и других науках. Я не говорил ничего подобного, и я не разделяю подобное мнение». Это беззастенчивое опровержение продержалось на сайте всего несколько дней. Под напором шквала национального про-

---

[1] «Information that was once available» (Информация, которая когда-то была доступна), *BBC News Online* от 5 октября 2001 года.

[2] Крис Шерман (Chris Sherman) «Deleted „Sensitive“ Information Still Available via Google» (Удаленная «чувствительная» информация все еще доступна в Google), *Search Engine Watch* от 9 октября 2001 года.

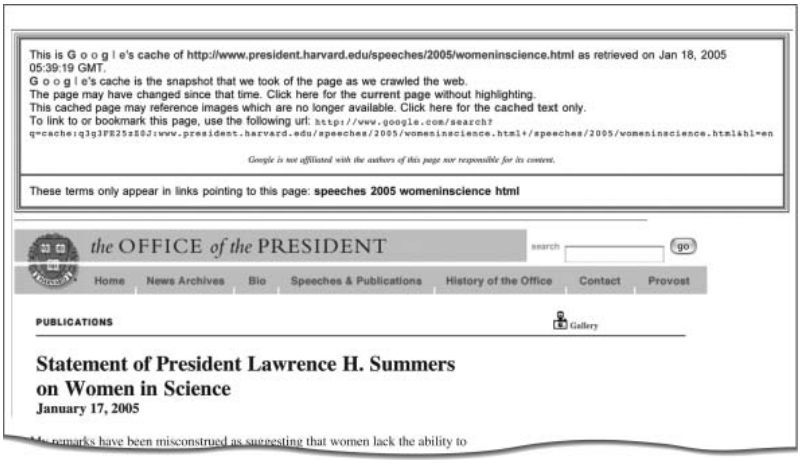


Рис. 4.3. *Часть кэшированной веб-страницы. Поисковая система* ***Google*** *сохранила копию официального заявления ректора Гарвардского университета, замененную через два дня после негативной реакции общественности. Эту копию выдала система* ***Google после исчезновения заявления с университетского веб-сайта.*** *Университет, обладающий авторскими правами на текст заявления, запретил его перепечатку в этой книге (см. заключение)*

теста ректор 19 января 2005 года выпустил новое заявление, в котором, в частности, сообщалось следующее: «Я глубоко сожалею о случившемся вследствие моих замечаний и приношу извинения за то, что недостаточно обдумал свои выражения». Те, кто искал в системе Google текст обращения ректора, получали ссылку на последнюю версию; но в течение некоторого времени стал доступен и первоначальный, оскорбительный, текст в виде копии из кэша поисковой системы.

Цифровая экспансия принесла возможность как мгновенной связи, так и мгновенного стирания; но почти каждый шаг в цифровом мире оставляет цифровые следы. Биты погибают не так-то легко, и цифровые слова, однажды произнесенные, бывает трудно вернуть в небытие.

Если Джен кэширует веб-страницы, то вы можете получить шанс ознакомиться с той информацией, которая была удалена вскоре после публикации из-за ошибочных действий или неудобства для ее автора. Кое-что в действиях Джен, однако, не совсем правильно. Авторское право еще никто не отменял, так что если у публикуемого материала есть автор, то вряд ли Джен можно хранить кэшируемую или какую бы то ни было копию, а также показывать ее другим. Разве у автора меньше прав распоряжаться своими произведениями, чем у того, кто делает копии?

Цифровое нашествие принесло с собой как возможность мгновенной связи, так и возможность мгновенного стирания; но почти каждый шаг в цифровом мире оставляет цифровые следы.

Этот вопрос вводит вас в мир проблем законодательства по защите авторских прав в цифровом веке; мы еще вернемся к этому в главе 6. Джен не может индексировать чью-то веб-страницу без получения ее копии. Более точно, каждый раз во время посещения страницы ваш броузер получает ее копию, которую затем визуализирует в окне. Еще один камень в огород определения Всемирной паутины как *библиотеки*.

Просмотр веб-страницы – это не пассивное наблюдение, это обмен битами в той степени, в какой это допускается сайтом. Если полностью защитить все веб-страницы от копирования, то ни поисковые системы, ни сама Всемирная паутина не смогут работать. Поэтому какое-то копирование должно быть разрешено. С другой стороны, когда Джен кэширует индексируемый материал – возможно, целую книгу, как в проекте Google Books, – появляется гораздо больше оснований для правового разбирательства. В конце концов, как будет сказано в главе 6, Ассоциация американских издателей (Association of American Publishers) и корпорация Google увязли в разбирательстве на предмет того, что корпорация может, а что не может делать с цифровыми сканированными копиями книг.

Обнаружение удаленных веб-страниц

Простейший эксперимент по обнаружению и просмотру удаленных страниц состоит в запросе к системе Google на предмет поиска проданного предмета в сервисе объявлений *craigslist.com*. Для поиска по определенному сайту нужно использовать ключевое слово «site:», примерно так:

```
предмет site:craigslist.com
```

Результат выполнения запроса, скорее всего, будет содержать ссылки на копии страниц, уже удаленных из сервиса, но сохраненных в кэше.

Шаг 3: формирование индекса

При обработке поискового запроса происходит обращение к индексу, базовая структура которого похожа на предметный указатель книги: список терминов и соотвествующих мест нахождения. Так же, как книжный указатель содержит номера страниц, индекс Джен содержит ссылки на веб-страницы (URL). Для того чтобы давать более подходящие ответы на запросы, индекс может содержать и другую информацию, например размер шрифта для данного термина или его положение на странице.

Индексы чрезвычайно важны, потому что должным образом упорядоченный индекс – как алфавитный индекс в книге – позволяет произво-

дить поиск гораздо быстрее, чем при последовательном сканировании. Именно здесь программисты Джен отрабатывают свой хлеб, находя новые эффективные решения такого хранения данных, чтобы поиск был наиболее быстрым. Закон Мура также внес свой вклад в решение данных задач – до тех пор, пока компьютерная память не стала достаточно емкой, быстрой и дешевой, даже изощренные программные решения не могли обеспечить удовлетворительную обработку произвольных запросов на естественном языке.

Когда Джен ищет слово в индексе, она не начинает поиск с начала с последующим просмотром всех терминов подряд. Указатель книги, к примеру, упорядочен по алфавиту, что позволяет искать нужное слово гораздо быстрее. Простой способ поиска нужного термина в объемном указателе, например, в телефонном справочнике, заключается в том, чтобы, открыв справочник на середине, решить, принадлежит ли искомый термин первой или второй половине указателя. Одна половина справочника отбрасывается, и тот же прием повторяется для оставшейся половины. Шагов поиска будет столько, сколько раз можно разделить количество страниц на два. Если в телефонной книге 1000 страниц, то чтобы найти нужную, понадобится применить описанный прием не больше 10 раз. Этот способ известен под названием алгоритма *бинарного (или двоичного) поиска*.

В общем случае число шагов алгоритма бинарного поиска по списку из n пунктов пропорционально числу степеней двойки в n. Скорость бинарного поиска экспоненциально возрастает по сравнению с линейной скоростью последовательного перебора: поиск среди миллиона терминов потребует не более 20 шагов, среди миллиарда терминов – не более 30 шагов.Довольно просто привести пример бинарного поиска в обычных человеческих действиях: если вы ищете в телефонной книге фамилию «Ледин», то надо открыть книгу где-то посередине, а если фамилию «Абельсон», то в начале. Есть еще более быстрые компьютерные алгоритмы поиска, скорость которых экспоненциально возрастает по сравнению со скоростью бинарного алгоритма.

Индексы и конкорданции

Информационная структура, применяемая поисковыми системами, называется обращенным индексом. Это список слов в документе или наборе документов с указанием на места, где эти слова встречаются. Идея обращенного индекса не нова; библиотечные указатели (конкорданции), старательно составленные средневековыми монахами, являются обращенными индексами. Создание обращенных индексов было одним из первых примеров приложения компьютерных технологий к нематематической задаче.

Насколько велик индекс Джен на самом деле? Для начала, сколько в нем терминов? Это еще одна коммерческая тайна Джен. Индекс Джен целесообразно использовать при наличии нескольких десятков миллионов терминов. В английском языке меньше полумиллиона слов, но Джен не откажется проиндексировать еще и некоторые числа (попробуйте указать в строке запроса вашей поисковой машины число, например 327). Еще неплохо бы добавить собственные имена, а также кое-какие иностранные слова. Список веб-страниц, ассоциированных с тем или иным термином, в большинстве случаев хранится на диске, а список самих терминов – в оперативной памяти. Если хранение термина и ассоциированных с ним ссылок на веб-страницы занимает 100 байт на запись, а число записей 2,5 миллиона, то индексная таблица займет в памяти 2,5 гигабайт (примерно 2,5 миллиарда байт). Еще несколько лет назад трудно было даже вообразить, что компьютер может быть оснащен оперативной памятью такого размера; в наши дни такой компьютер можно заказать в розничной сети, например Wal-Mart.

Поиск по индексу в оперативной памяти может происходить быстро (например, при помощи алгоритма бинарного поиска), но получение списка ссылок (URL) может потребовать обращения к диску. Если бы Джен обладала ресурсами Google, она могла бы ускорить выдачу ответа, сохраняя в оперативной памяти и ссылки, а чтобы повысить производительность еще больше, Джен могла бы распределить процедуру поиска между несколькими компьютерами.

Сегодня мы можем сами оценить эффективность указанных мер, наблюдая скорость работы реальных поисковых систем.

Шаг 4: разбор текста запроса

Когда авторы ввели в строку поиска системы Google запрос «Yankees beat Red Sox» (Yankees победили Red Sox), то лишь одна из пяти верхних ссылок страницы результатов указывала на победу бейсбольной команды Yankees (рис. 4.4). Другие указывали на победу команды Red Sox. Это случилось потому, что компьютеры с трудом вострнимают естественный (человеческий) язык, а также потому, что его фразы могут быть неоднозначны. Поэтому поисковая система рассматривает фразы как набор слов и ищет в индексе ссылки на страницы, содержащие все слова. Это требует менее сложных вычислительных операций, хотя смысл фразы может быть потерян.

Чтобы уменьшить влияние языковых неоднозначностей, поисковая система предлагает пользователям возможность составлять *расширенные запросы* (advanced queries), позволяющие более тонко настроить поисковый алгоритм. Даже самый простой вариант – заключение фразы в двойные кавычки (“ “) – используют меньше 10% пользователей поисковых систем. Заключение фразы «Yankees победили Red Sox» в двойные кавычки в строке поиска дает более адекватные результаты.

Рис. 4.4. *Поиск по ключевым словам приводит к потере значения фразы в целом. Большинство результатов поиска системой* ***Google ответа на запрос «Yankees beat Red Sox» указывают на обратное – победу команды Red Sox***

Google™ является зарегистрированной торговой маркой. Перепечатка с разрешения корпорации Google

Также в Google возможно использовать знак тильды (~): если поместить его перед словом, поисковая система будет просматривать синонимы; знак дефиса (-) требует показывать ссылки на страницы, не содержащие следующее за ним слово; есть и целые команды, например «allinurl:» или «inanchor:», позволяющие ограничить область поиска. Строго говоря, наш исходный запрос был едва ли корректным, но большинство пользователей просто вводят набор слов и получают удовлетворительные результаты.

Нередко результат поиска может довольно сильно отличаться от ожидаемого. Запросите у поисковой системы Yahoo! слова «allergy» и «treatment» («аллергия» и «лечение») и получите больше 20 миллионов ссылок. Если вы заключите оба слова в кавычки – «allergy treatment» («аллергия лечение»), – то получите 628 тысяч ответов и уже другие верхние строчки. Наконец, фраза в кавычках «treating allergies» («лечение аллергий») сократит список до 95 тысяч. Разница между всеми запросами может показаться незначительной для вас, но существенной для поисковой системы. Просто удивительно, насколько полезным может оказаться общение человека с компьютером посредством поисковой системы, даже несмотря на ее очевидные недостатки!

Сегодня пользователи стараются терпеливо относиться к ошибкам поисковых систем. Считая причиной ошибок себя, пользователи составляют более эффективные запросы. Может быть, это вызвано непрекращающимся удивлением людей по поводу того, что эти штуки (поисковые системы) вообще работают. Имеет смысл проявлять терпение, так как затраты пользователя, связанные с неправильными ответами, обычно невелики. Но по мере усовершенствования технологий пользователи будут ожидать большего и станут менее терпимы к бесполезным ответам поисковых систем.

Запросы на естественных языках

Технология разбора запросов на естественных языках непрерывно совершенствуется. К примеру, экспериментальный сайт *www.digger.com* укажет вам недостатки вашего запроса и поможет их исправить. Если вы запросите у сайта информацию по «java», сайт уточнит, имели вы в виду напиток (кофе), остров Ява (Java) или одноименный язык программирования, а затем выдаст адекватный ответ.

Сайт Powerset (*www.powerset.com*) использует программное обеспечение для разбора запросов на естественном (английском) языке и выдает соответствующие ответы в зависимости от содержимого веб-страниц. Этот сайт может корректно обработать фразу «Yankees beat Red Sox».

Современные исследования ведут к тому, что программное обеспечение научится правильно разбирать запросы на естественных языках до того, как пользователи приведут свое сознание в соответствие машинной логике. Но это вряд ли случится в обозримом будущем. Возможно, при стократном увеличении производительности компьютеров семантический разбор содержимого веб-страниц станет настолько качественным, что загадочных ответов на простые запросы просто больше не будет.

Шаг 5: определение адекватности каждого из полученных результатов

Работа поисковой системы состоит в том, чтобы обеспечить результаты, соответствующие содержанию строки запроса. На техническом жаргоне критерий степени совпадения называется *релевантностью*. Релевантность включает объективный компонент – повествование о победе команды Red Sox над Yankees является едва ли верным ответом на запрос «Yankees победили Red Sox». Релевантность также содержит и субъек-

тивный компонент, так как только автор запроса в конечном счете оценивает степень адекватности ответов поисковой системы. Возможно, в запросе имелась в виду команда Yankees из Нью-Йорка, одержавшая победу над бостонской командой Red Sox из Главной лиги бейсбола, а может быть, автор в этот момент думал о командах Yankees из Флагстафа и Continental Red Sox из Малой лиги бейсбола штата Аризона.

Нахождение всех релевантных документов называют *повторным вызовом* (recall). В связи с колоссальным объемом Всемирной паутины нет надежного способа убедиться, что поисковая система нашла все адекватные ответы. Полный повторный вызов недостижим, да и не нужен. Джен может найти тысячи или даже миллионы ссылок в своем индексе, но пользователя едва ли заинтересуют больше одной-двух. Степень релевантности всегда ограничивает масштаб повторного вызова. Пользователи желают получить хорошие ответы, а не множество их.

Поисковые системы и выборка информации

В этих трех статьях высказываются интересные взгляды на принципы работы поисковых систем и технологии выборки информации:

Статья основателей корпорации Google Сергея Брина (Sergey Brin) и Ларри Пейджа (Larry Page) «The Anatomy of a Large-Scale Hypertextual Web Search Engine» (Анатомия широкомасштабной гипертекстовой поисковой системы), 2000[1] подробно рассматривает принципы и цель работы поисковой системы Google и ее отличие от более ранних аналогов.

Статья Амита Сингала (Amit Singhal) «Modern Information Retrieval: A Brief Overview» (Современный информационный поиск: краткий обзор), 2001[2] – обзор достижений в сфере информационного поиска. Амит Сингал учился у Дж. Салтона, а сейчас является руководителем команды ранжирования корпорации Google.

Статья профессора информатики университета Иллинойса Дэвида Дабина (David Dubin) «The Most Influential Paper Gerald Salton Never Wrote» (Самая важная работа Джеральда Салтона не была написана)[3] открывает неожиданные стороны основ науки информационного поиска.

---

1 *infolab.stanford.edu/~backrub/google.html*

2 IEEE Data Eugineering Bulletin, 24(4), с. 35–43, 2001.

3 «Library Trends», весна 2004 г., *findarticles.com/p/articles/mi_m1387/is_4_52/ai_n7074022*.

Наука измерения релевантности много старше Всемирной паутины. Оценка релевантности берет начало в 1960-х, в работе Джеральда Салтона (Gerald Salton), вначале в Гарвардском университете, а затем в Корнелльском. Суть проблемы в том, что автоматизация действия, учитывающего количество успешных попаданий в каком-либо процессе, сильно подвержена субъективной оценке. Ожидается, что компьютер просканирует документ, осуществит разбор запроса, выполнит некоторые вычисления и выдаст некоторое числовое значение критерия релевантности документа по отношению к запросу.

Приведем простейший пример подсчета релевантности документа запросу. Предположим, в языке насчитывается 500 тысяч слов. Создадим два списка из 500 тысяч позиций, по одному списку для документа и для запроса. Каждая позиция в списках соответствует одному слову, к примеру № 3682 обозначает «лекарства». Для списка документа каждая позиция содержит число раз, когда соответствующее слово встречается в тексте. То же самое и для запроса – если в нем нет повторов, то в списке запроса будет встречаться либо 0, либо 1. Перемножим числа в соответствующих позициях обоих списков и сложим полученные произведения. Если ни одно из слов запроса не встречается в документе, то результат будет равен 0, иначе – отличен от 0. Чем чаще слова из запроса будут встречаться в документе, тем больше конечный результат.

На рис. 4.5 показано, как производится вычисление релевантности для запроса «Yankees beat Red Sox» и видимой части третьего документа с рис. 4.4, начинающегося словами «Red Sox rout Yankees» («Red Sox разгромили Yankees»). (Другие, возможно, содержат больше ключевых слов в полном документе.) Позиции в двух списках соответствуют терминам из словаря в алфавитном порядке, от A до Z. Слова «red» и «sox» появляются во фрагменте по два раза, а название «Yankees» – трижды.

Этот метод подсчета довольно груб, и его недостатки очевидны. Объемные документы получат более высокое значение релевантности, чем краткие, так как содержат больше повторов. Незначащие слова, например, предлоги, вносят свой вклад в расчет наравне с важными терминами, например, именами собственными. В дополнение к частоте и многообразию слов поисковые системы Google, Yahoo!, MSN и Ask.

Lexicon:	ant, …,	beat, …,	defeating, …,	new, …,	patriots, …,	red, …,	sox, …,	Yankees, …,	zebra, …
Doc:	0, …,	1, …,	2, …,	1, …,	0, …,	2, …,	2, …,	3, …,	0, …
Query:	0, …,	1, …,	0, …,	0, …,	0, …,	1, …,	1, …,	1, …,	0, …
Doc × Query	0, …,	1, …,	0, …,	0, …,	0, …,	2, …,	2, …,	3, …,	0, …

Sum of elements of Doc × Query = 1+2+2+3 = 8 = “relevance” of document to query

Рис. 4.5. *Списки документа и запроса для расчета релевантности*

com учитывают и многие другие факторы. Могут применяться весовые коэффициенты, то есть слова, вынесенные авторами документов в заголовки или выделенные иначе, вносят больший вклад в общую сумму. Пользователи, как правило, печатают наиболее важные слова в начале запроса, так что «вес» термина может зависеть от его позиции в строке поиска.

Шаг 6: определение приоритетности полученных результатов (ранжирование)

После того как Джен выбрала релевантные документы – допустим, что поисковая система выбрала все документы с релевантностью, достигшей заданного порога, – она «ранжирует» (rank) полученный набор, то есть упорядочивает его. Ранжирование очень важно для установления ценности результатов поиска. Джен может найти тысячи релевантных результатов, но пользователям нужно лишь несколько. Простейшее ранжирование производится по значению релевантности – страницы с большими значениями указываются в начале. Этот метод, однако, работает не лучшим образом. Для коротких запросов значение релевантности примерно одинаково у множества документов. Ссылки, предоставляемые Джен пользователям, должны быть «хорошими» – то есть представленные документы должны не только обладать заданным значением релевантности, но и отвечать желаниям пользователей. Это трудно определимое соответствие можно назвать «качеством» ответа Джен. В приведенном выше примере поиска по запросу «spears» кто-то должен принять решение, почему ссылки на документы о поп-звезде Бритни Спирс должны быть «лучше», чем ссылка на личный сайт профессора Спирса. И чем бы ни было это «качество», процесс ранжирования для основных поисковых систем происходит автоматически и без участия пользователей. Пока не существует информационных протоколов для оценки профессиональных лицензий или наличия судимостей – по крайней мере, в нынешней Всемирной паутине.

Измерить «качество» веб-страницы нельзя, но путем анализа взаимосвязей во Всемирной паутине для нее можно сформировать что-то вроде «значимости» или «репутации». Приближенной аналогией могут быть научные публикации. Научная репутация авторов тем выше, чем больше ссылок на их работы приводится в публикациях других работников науки. Эта система, конечно, не идеальна – существуют и «псевдонаучные» журналы, и околонаучные сообщества, поддерживающие свое существование посредством взаимных восхвалений. Однако во Всемирной паутине анализ структуры ссылочных связей – хорошая отправная точка для измерения значимости веб-страниц.

Одним из нововведений корпорации Google в области поиска стала оценка релевантности с помощью некоторой числовой величины, называемой PageRank. Величина PageRank показывает «значимость» веб-страницы в зависимости от количества ссылок на нее на других

сайтах – контекст популярности страницы в Интернете. Логика такова, что чем больше ссылок, тем выше «значимость». Также величина PageRank увеличивается в зависимости от того, насколько *велика* «значимость» ссылающихся страниц. Такой подход, если упустить это из виду, может создать закольцованное взаимное повышение величины PageRank, но эту проблему можно решить – требуется лишь немного математики и большая вычислительная мощность.

Что способствует нахождению веб-страницы

Ни одна компания-владелец поисковой системы не разглашает свои секреты вычисления релевантности и ранжирования. Алгоритмы хранятся в тайне, потому что являются конкурентным преимуществом, а также потому, что знание алгоритма будет способствовать появлению в Интернете веб-страниц с высокой степенью релевантности, но, скорее всего, бесполезных по содержанию для пользователей. Однако есть некоторые общеизвестные детали:

- значимость ключевого термина зависит от его нахождения в заголовке веб-страницы или html-заголовке первого или второго уровня;
- имеет значение частота упоминания ключевого термина в основном тексте;
- «доверенные» сайты анализируются иначе, чем обычные;
- попутно оценивается релевантность связанных ссылками страниц;
- имеет значение «возраст» веб-страницы»;
- то же для связанных страниц;
- на оценку влияют объективные факторы, например орфографические ошибки в тексте страницы.

Если вы хотите погрузиться в исследование принципов работы поисковых систем, то найдете множество факторов для анализа – вам лишь останется позаботиться о том, чтобы хватило вычислительной мощности!

Способ ранжирования на основе количества ссылок, похоже, учитывает репутацию и свободен от пристрастий – это просто автоматизированный подсчет взаимных мнений. К примеру, когда авторы искали в поисковой системе Google «лекарства от шизофрении», верхний результат ответа был ссылкой на раздел сайта шведского университета. Определенно, выбор поисковой системы основывался на релевантности: страница была посвящена проблеме лечения шизофрении, а слова запроса располагались в заголовке страницы. Поэтому если бы запрос

содержал другие слова, то и результат поиска был бы другим. Порядок слов также имеет значение – поисковый алгоритм Google возвращает разные ответы на запросы «drugs schizophrenia» («шизофрения лекарства») и «schizophrenia drugs» («лекарства от шизофрении»).

Эта страница могла попасть в начало списка результатов поиска еще и потому, что на нее ссылались другие страницы, в особенности если их собственная значимость была высокой. Другие веб-страницы могли иметь лучший стиль текста, быть созданы более авторитетными учеными, содержать более свежую информацию или меньшее число фактических ошибок. Обо всех этих свойствах страниц поисковый алгоритм судить не может, и никто из сотрудников корпорации Google не читает все страницы подряд, чтобы выносить суждения.

Поисковая система Google и ее конкуренты применяют собственные секретные методы автоматического ранжирования. Подобно формуле кока-колы, детали коммерческих алгоритмов известны лишь немногим людям. Алгоритм ранжирования Google PageRank запатентован, поэтому доступно лишь его краткое описание. На рис. 4.6 представлена иллюстрация из патентного документа, на которой показаны несколько страниц, содержащих ссылки друг на друга. Предполагается, что как страницам, так и ссылкам в зависимости от их значимости могут быть присвоены числовые значения. В описании опущены многие детали, а практическая реализация алгоритма непрерывно совершенствуется. Единственное значение для владельца поискового сервиса имеет рабо-

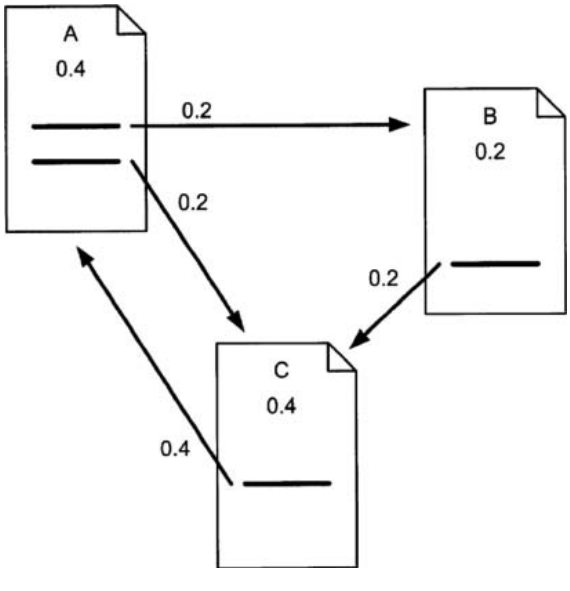


Рис. 4.6. Иллюстрация из патентного документа Google PageRank (Патентное бюро США, документ U.S. Patent #6285999), на которой показано, как взаимные ссылки документов могут получать различные числовые значения

тоспособность функции ранжирования, в том смысле что пользователи довольны результатами. Если результат не устраивает пользователей, они будут использовать другие поисковые системы.

Во время разработки прототипа поисковой системы Google ее создатели, Сергей Брин и Ларри Пейдж, были аспирантами Стэнфордского университета. Корень «Page» в слове «PageRank» происходит не от веб-страницы (web page), а от фамилии одного из создателей (Larry Page).

Людям нравится думать о предпочитаемых ими поисковых системах, что те могут в любое время предоставить точную, полезную и даже достоверную информацию. Но «говорить только правду и ничего, кроме правды» для поисковых систем является всего лишь средством достижения конечной цели – обогащения компании-владельца.

Ранжирование страниц – дело вкуса. Но от правильного выбора зависит многое. Для пользователя обычно не столь важно, какой из ответов появится в первой строчке ответа или даже насколько представленные ссылки соответствуют запросу. А вот для компании, предлагающей на сайте свою продукцию, место и значимость в индексе поисковой системы могут быть вопросом жизни и смерти.

Компания KinderStart владеет сайтом *www.kinderstart.com*, который содержит каталог и поисковый сервис товаров и услуг для детей. 19 марта 2005 года посещаемость сайта понизилась на 70 %, после того как система Google понизила значение PageRank сайта до ноля (по шкале от 0 до 10).[1] Возможно, поисковый алгоритм Google понизил значимость сайта из-за того, что содержимое его страниц представляло собой, главным образом, ссылки на другие сайты. Общедоступное описание критериев оценки алгоритма ранжирования Google содержит предупреждение насчет страниц «с незначительным оригинальным содержимым или отсутствием такового».[2] Компания KinderStart придерживалась своей точки зрения на содержимое сайта и возбудила судебное дело против корпорации Google. Среди прочего, в заявлении корпорация Google обвинялась в нарушении права компании на свободу слова в соответствии с Первой поправкой к Конституции США, что выражалось в фак-

[1] В соответствии с заявлением Kinderstart о запрещающих и объяснительных мерах и убытках; федеральный суд Северного округа штата Калифорния, отделение Сан-Хосе, дело № C 06-2057 RS, 17 марта 2006 года, *blog.ericgoldman.org/archives/kinderstartgooglecomplaint.pdf*.

[2] Центр справки Google для веб-мастеров, «Незначительное наличие или полное отсутствие оригинального содержимого», *www.google.com/support/webmasters/bin/answer.py?answer=66361*.

тической «невидимости» сайта для поисковой системы (а следовательно, неинформированности пользователей). Корпорация ответила тем, что низкое значение PageRank является лишь ее собственным мнением, которое не может быть предметом судебного разбирательства:

> Поисковый сервис Google, как и любой другой, выполняет свою функцию оценки для удобства пользователей, руководствуясь своими принципами и выражая свое мнение об относительной значимости веб-сайтов тем способом, который сделал поисковую систему Google выбором миллионов пользователей. Судебный представитель компании KinderStart настоял на том, чтобы суд вынес окончательное решение по этому принципиальному вопросу.[1]

Компания KinderStart не согласилась с тем, что значение PageRank является лишь собственным мнением корпорации Google. «Величина PageRank является чем-то иным, нежели выражением мнения, вызванного собственной оценкой или жалобой человека на данный веб-сайт или его отдельные страницы... Это математически полученный результат измерения и нахождения количества и глубины всех гиперссылок во Всемирной паутине, связанных с оцениваемым веб-сайтом, в соответствии с программным заявлением представителя корпорации Google», – заявил представитель компании.[2]

Судья отклонил все доводы компании KinderStart, в том числе обвинение в нарушении ее права на свободу слова, обвинение корпорации Google в монополизации рынка поисковых услуг, а также заявление о попытке дискредитации компании-истца путем понижения до ноля значения PageRank ее веб-сайта.

Как узнать значение PageRank конкретной веб-страницы?

Для этого корпорация Google предлагает использовать фирменную панель инструментов для броузера, доступную для скачивания по адресу *toolbar.google.com*. Другой способ состоит в посещении сайта *www.iwebtool.com/pagerank_checker*: для получения значения PageRank нужно ввести URL-адрес нужной страницы.

---

[1] Эрик Голдман (Eric Goldman) «Google's motion to dismiss Kinderstart lawsuit» (Действия Google по отклонению иска Kinderstart), *blog.ericgoldman.org/archives/2006/05/kinderstart_v_g.htm*.

[2] Иск Kinderstart.com LLC от своего имени и имен тех, кто оказался в аналогичной ситуации, против Google. Федеральный суд Северного округа штата Калифорния, дело № C 06-2057 JF (RS), решение судьи Джереми Фогеля, 13 июля 2006 года.

Неизвестно, является ли это «мнением» или «попыткой дискредитации», но сайт компании KinderStart определенно легче найти с помощью поисковой системы Yahoo!. Там при запросе «kinderstart» сайт появляется в первой строчке результатов поиска, а в поисковой системе Google – только на двенадцатой странице.

Подобная судьба постигла *bmw.de* – сайт немецкого автопроизводителя BMW. Страница, проиндексированная Google, содержала выражения «gebrauchtwagen» и «neuwagen» («подержанный автомобиль» и «новый автомобиль»), повторяющиеся десятки раз.[1] Уловка разработчиков позволила скрыть это содержимое от пользователей, которые видели довольно комфортный дизайн с небольшим количеством текста и множеством изображений.[2] Цель уловки заключалась в поднятии значимости сайта в ответах на запросы типа «подержанный автомобиль» и «новый автомобиль». Разработчики пренебрегли ясными инструкциями корпорации Google: «Создавайте страницы в первую очередь для пользователей, а не для поисковых систем. Не вводите пользователей в заблуждение и не публикуйте разное содержание: одно для поисковых систем, а другое – для пользователей. Маскирование (а это называется именно так) не приветствуется».[3] Корпорация Google ответила на уловку «высшей мерой наказания» – исключением сайта *bmw.de* из индекса. Какое-то время сайт еще пытался существовать во вселенной Google. Принятые меры показали, что корпорация Google готова к решительным действиям против сайтов, пытающихся поднять свою значимость нечистоплотным способом. Также стало ясно, что от исключения из индекса *не застрахован* ни один сайт.

Шаг 7: представление результатов

После всей огромной и утомительной работы, проделанной на шагах 1–6, поисковые системы обычно предлагают пользователю результат в форме, которая старше самого Аристотеля, – в виде простого списка. Но встречаются и менее примитивные способы представления.

Если вы ищете нечто расплывчато-неопределенное, вроде «чистка», в одной из крупных поисковых систем, то получите миллион результатов: от стиральных машин до антивирусных программ. На сайте Home Depot вы при том же запросе получите более удобный для поиска набор

---

[1] Блог Мэтта Каттса (Matt Cutts) «Gadgets, Google, and SEO, Ramping up on international webspam» (Гаджеты, Google и поисковая оптимизация на вершине волны международного интернет-спама), 4 февраля 2006 года, *www.mattcutts.com/blog/ramping-up-on-international-webspam/*.

[2] «BMW given Google ‘death penalty’» (Google назначает BMW «высшую меру наказания»), *BBC News* от 6 февраля 2006 года, *news.bbc.co.uk/1/hi/technology/4685750.stm*.

[3] Центр справки Google для веб-мастеров, *www.google.com/support/webmasters/bin/answer.py?hl=en&answer=35769*.

Рис. 4.7. *Страница результатов поиска по запросу «чистка» (**«washers»**) на сайте **Home Depot***

Источник: сайт торговой сети товаров для дома Home Depot, www.homedepot.com

категорий, цен, производителей и других понятий, сопровождаемых к тому же изображениями (рис. 4.7).

Альтернативы простому ранжированному списку при представлении результатов дают большую наглядность. Использование новых форм навигации может изменить баланс сил в уравнении поиска. Верхняя позиция в списке результатов может больше не иметь прежней экономической ценности; текущий всеобщий критерий значимости способно вытеснить нечто иное, например качество изображений. Кроме того, вне зависимости от способа представления большинства результатов есть и дополнительные элементы представления, которые появляются рядом с основными (ранжированными). Настало время обсудить рекламные (или спонсорские) ссылки.

Кто и за что платит?

Веб-поиск – одна из наиболее широко используемых функций компьютеров. Более 90% взрослых пользователей Интернета используют поисковые системы, более 40% из них делают это ежедневно.[1] Популярность поисковых систем легко объяснить. Как правило, это бесплатно. Не нужно проходить процедуры регистрации, читать пользовательские соглашения, настраивать параметры соединения и даже утечка персональной информации вроде бы не наблюдается. Если вы подключены к Интернету, то, скорее всего, у вас есть веб-броузер; возможно, он уже настроен на автоматическое подключение к поисковой системе при запуске. Не нужно изучать инструкции, по крайней мере, для начала работы. Просто наберите несколько слов в строке поиска и изучайте результаты. Вы не можете никому навредить, набирая фантастические запросы и наблюдая реакцию поисковой системы. Это даже забавно.

Возможно, именно простота и доступность веб-поиска заставляют нас сравнивать его с общедоступными услугами – это что-то вроде комбинации энциклопедии и уличного фонаря, единого источника знаний и направлений, помогающего каждому. С экономической точки зрения, это плохая аналогия. Общественные службы берут с вас плату за предоставление, к примеру, воды, газа или электричества, а поисковые системы – нет. Общественные службы нечасто конкурируют, а поисковые системы – постоянно.

Еще люди доверяют поисковым системам, потому что их услуги (как и коммунальные удобства, к примеру) просто доступны в любое время и обычно соответствуют ожиданиям. Если запросить у поискового сервиса информацию по авиакомпании American Airlines, то сайт компании тут как тут, а если кого-то интересует «the price of tea in China» (цена на чай в Китае), найдется и цена (1 доллар 84 цента за 25 пакетиков), и вариант толкования фразы. Возможно, часть доверия поисковым системам происходит от уверенности в их беспристрастности как программ. Все же то, что люди редко разочаровываются в этих предположениях, еще не означает их абсолютную правильность.

Кто же оплачивает все эти удобства? Есть четыре варианта:

- платят пользователи (например, как подписчики);
- платят сайты за право попасть в индекс;
- платит правительство или некоторая некоммерческая организация;
- платят рекламодатели.

Были испытаны все четыре модели оплаты.

---

[1] «Digital Footprints» (Цифровые следы), «Online identity management and search in the age of transparency» (Управление сетевой идентификацией и поиск в век открытости), Pew Internet & American Life Project, 2007, *www.pewinternet.org*.

Некоммерческий поисковый сервис

В начале пути сервис веб-поиска спонсировался правительством и университетами, через которые, собственно, и проходила львиная доля потока битов, в рамках грантов и исследовательских программ. Одной из первых технологий индексирования Всемирной паутины был исследовательский проект аспиранта факультета информатики Брайана Пинкертона (университет Вашингтона) под названием WebCrawler. Принципы проекта были опубликованы в статье на одной из первых конференций по Всемирной паутине в 1994 году.[1] В 1997 году появилась статья основателей Google о принципе назначения веб-страницам оценки PageRank[2], встретившая поддержку Национального научного фонда, Агентства по перспективным научно-исследовательским разработкам Департамента обороны, Национального управления США по аэронавтике и исследованию космического пространства (National Aeronautics and Space Administration, NASA), а также нескольких представителей промышленности, спонсирующих исследовательские программы в области информатики Стэнфордского университета. Патент на алгоритм PageRank на самом деле принадлежит Стэнфорду – корпорация Google всего лишь исключительный лицензиат.[3]

Научные и правительственные источники финансировали разработку и существование поисковых систем до тех пор, пока Всемирная паутина не стала средством ведения бизнеса. Для развития поисковым сервисам нужны были деньги. Некоторые сервисы подписки на услуги связи, такие как AOL, предлагали в списке услуг функцию поиска. Еще до того как поисковые системы получили распространение, на веб-страницах появились рекламные изображения (баннеры). Само собой, баннеры заняли свое место и в системах поиска информации. Баннеры эквивалентны доскам объявлений или рекламным модулям газет. Рекламодатель покупает себе немного места, и вот уже страница поиска заполняется соблазнительными обещаниями.

С появлением систем веб-поиска появилась и контекстная реклама, которая была видна только потенциально заинтересованным пользователям. К примеру, баннер фирмы, торгующей сотовыми телефонами,

---

[1] Брайан Пинкертон (Brian Pinkerton) «Finding What People Want» (Найти то, что нужно пользователям), Вторая международная конференция по Всемирной паутине, *thinkpink.com/bp/WebCrawler/WWW94.html*.

[2] Сергей Брин и Лоренс Пейдж (Sergey Brin and Lawrence Page) «The Anatomy of a Large-Scale Hypertextual Web Search Engine» (Анатомия широкомасштабной гипертекстовой поисковой системы), кафедра информатики Стэнфордского университета, 1997, *infolab.stanford.edu/~backrub/google.html*.

[3] Патент США #6285999 «Method for node ranking in a linked database» (Метод ранжирования узлов реляционной базы данных), подшит 9 января 1998 года, выдан 4 сентября 2001 года. Изобретатель: Лоренс Пейдж; патентовладелец: Совет попечителей Университета имени Леланда Стэнфорда-мл.

мог быть показан на странице результатов тем пользователям, которые ввели в строке поиска слово «телефон». Как и доски объявлений, рекламные баннеры приносят доход; излишнее количество объявлений или баннеров может утомить и оттолкнуть читателя.

Предполагается общепризнанный этический подход. Взяточничество здесь не приветствуется.

Какая бы бизнес-модель ни использовалась, предполагается общепризнанный этический подход. Предлагая пользователям поисковый сервис, вы не должны брать плату за изменение представления результатов. Если вы предлагаете информацию, то ожидается, что информация будет полной, хотя бы и субъективной. Взяточничество здесь не приветствуется. Есть грань между полнотой и субъективностью, но эта линия проходит по обширной и неисследованной территории. Область поиска непрерывно расширяется с тех пор, как научные и правительственные центры передали управление Интернетом в руки владельцев розничных сетей, торговцев недвижимостью и производителей лекарств.

Коммерциализация поисковых систем порождает дилемму – то, что Сергей Брин и Ларри Пейдж назвали в своей статье «смешанными мотивами» поисковых сервисов, построенных на рекламе. Как отреагируют рекламодатели на появление в результатах поиска высокоранжированных страниц, явно направленных против рекламируемых товаров? Брин и Пейдж привели пример, когда поиск по запросу «сотовые телефоны» возвращает статью об опасности разговора по сотовому телефону при вождении автомобиля. Станут ли производители средств связи платить за то, чтобы их реклама появилась рядом с *такой* информацией? Сергей Брин и Ларри Пейдж предостерегали, что «поисковые системы, основанные на рекламировании, по самой своей сути будут отдаляться как от ожиданий рекламодателей, так и от нужд пользователей». Также был приведен пример с поисковым сервисом Open Text, который вылетел из бизнеса после того, как стало известно, что сервис повышал значимость части сайтов за плату.

Размещения, переходы и аукционы

Год спустя мир изменился. Запущенный в 1998 году сервис Overture (сайт *GoTo.com*) зажил полноценной жизнью, решив этическую проблему собственным способом. Этическая грань оказалась лишь плодом воображения ученых мужей. Сервис Overture просто давал рекламодателям возможность быть найденными, и тем скорее, чем больше они были готовы заплатить. Главный смысл идеи состоял в том, что если кто-то готов платить за рекламу, то тот, кто платит больше, возможно, действительно ценнее для общества. Не имело значения, насколько это было логично или возмущало пуристов. Похоже, подход сработал, и люди были довольны. Генеральный директор сервиса Overture ясно изложил принцип работы сервиса. Считая каждый бит чем-то вроде

посредника на рынке, директор Джеффри Брюйер пояснил: «Честно говоря, никто до конца не знает, как любой отдельно взятый поисковый сервис формирует свои результаты. Если пользователи довольны, то механизм формирования их и не интересует».[1]

Пользователи в самом деле были довольны. Бурное развитие Интернета в конце 1990-х породило у коммерческих сайтов стремление быть видимыми повсюду, в то время как пользователи все чаще обращались для удовлетворения своих потребностей к Всемирной паутине. Сервис Overture внедрил еще одно нововведение, расширившее долю сервиса на сегмент сайтов, не обладающих достаточным бюджетом для оплаты дорогой рекламы на площадках Yahoo! или AOL. Нововведение заключалось в том, что за размещение рекламных ссылок средствами сервиса Overture плата не взималась. Рекламодатели должны были оплачивать только переход пользователя по рекламной ссылке. Для низкобюджетных интернет-компаний это была возможность покупать весьма недорогую рекламу. Поскольку оплата одного перехода была ничтожной, владельцы сайтов выстраивались в очередь на покупку новой услуги «плата-за-переход» («pay-per-click», PPC). Конечно, никто не мог рассчитывать на продажи с каждого перехода, но, по крайней мере, рекламодатели платили за пользователей, которые потрудились проявить интерес и узнать немного больше, чем можно было уместить на баннере.

Когда определенные ключевые слова поиска стали популярны, цены на оплачиваемые ссылки стали расти. Сервис Overture внедрил третье нововведение, как способ формирования цен. Если несколько рекламодателей претендовали на одно место на веб-странице, сервис Overture проводил между ними аукцион. Цена на рекламную площадку могла доходить до одного доллара за переход. Цена перехода колебалась в зависимости от количества участников аукциона, боровшихся за право быть найденными по определенным ключевым словам. Если на странице поиска по ключевому слову, например «фотокамера», хотело появиться много рекламодателей, то цена за переход возрастала. Рекламная площадь на экране – ограниченный ресурс, а рынок диктует свою цену. Сервис распродажи ключевых слов прост, поддается расчету и очень выгоден.

По иронии судьбы взрыв интернет-пузыря в 2000 году сделал модель бизнеса сервиса Overture еще более заманчивой. После крушения надежд и капиталов многих интернет-компаний последние больше не могли позволить себе тратиться на покупку рекламных баннеров, значительная часть которых почти не приносила отдачи. В результате множество компаний переориентировались на предложения поисковой системы Overture и ее подражателей. Крах доткомов также задел сотни поисковых систем того времени. Когда конкуренция стала ощутимой, компании Yahoo! и AOL начали брать плату за места в списках результатов поиска.

---

[1] Дэнни Салливан (Danny Sullivan) «GoTo Going Strong, Search Engine Watch» (По оценке Search Engine Watch, сервис GoTo набирает силу), 1 июля 1998 года, *http://searchenginewatch.com/showPage.html?page=2166331*.

Дядя Сэм делает заметки

Разные поисковые сервисы предоставляли рекламодателям различные уровни открытости при показе их ссылок. Сервис Yahoo! помечал оплаченные ссылки словом «Sponsored» (оплачено), ставшим общепризнанным обозначением для оплаченной рекламы. Другие поисковые системы употребляли более расплывчатые определения, например «partner results» (партнерские результаты) или «featured listings» (списки с дополнительными возможностями). Руководство сервиса MSN корпорации Microsoft придумало очень «остроумное» оправдание термину «featured»: исследования разработчиков MSN показали[1], что пользователи, оказывается, уже осведомлены о том, что результаты поиска заранее оплачены – так что в дополнительном оповещении пользователей нет никакой необходимости! По мере увеличения числа дорожных жертв на скоростной магистрали информационного движения бизнес в сети становится все менее забавным, а деловые практики все меньше отвечают духу свободы, породившему Интернет. «Мы больше не можем себе позволить участвовать в идеологических дебатах, – заявил руководитель одного из интернет-проектов Эван Торнли. – Мы публичная компания».[2]

Первоначально за порядком в Интернете следило правительственное агентство, но в 2001 году к делу подключилась Consumer Alert, активистская организация адвоката Ральфа Нейдера. Совместно с Федеральной торговой комиссией организация подготовила документ, сообщающий, что 8 поисковых сервисов участвовали в обмане пользователей, помещая оплаченные ссылки вместе с найденными поисковым алгоритмом без возможности различения.

Исполнительный директор Consumer Alert Гари Раскин высказался прямо: «Эти поисковые сервисы отказались от познавательной целостности в угоду бездушной гонке за капиталом. Мы просим Федеральную торговую комиссию проследить за тем, чтобы никто более не подвергался риску быть обманутым поисковыми системами, опустившимися до делового жульничества. Если они собираются помещать рекламные материалы в результатах поиска, то необходимо обязательно указывать, где реклама, а где – нет».[3]

---

[1] Верн Копытофф (Verne Kopytoff), «Searching for profits: Amid tech slump, more portals sell search engine results to highest bidder» (Поиск ради прибылей: посреди технического переполоха все больше порталов перепродают результаты поиска тем, кто больше заплатит), *San Francisco Chronicle* от 18 июня 2001 года.

[2] Там же.

[3] «Commercial Alert возбуждает дело против поисковых систем, создающих мошенническую рекламу», веб-сайт Commercial Alert, 16 июля 2001 года, *www.commercialalert.org/news/news-releases/2001/07/commercial-alert-files-complaint-against-search-engines-for-deceptive-ads.*

Рис. 4.8. *Извещение Федеральной торговой комиссии США о рекламных ссылках в списках результатов поисковых систем*

Источник: Федеральная торговая комиссия США

Федеральная торговая комиссия удовлетворила прошение, обязав владельцев поисковых систем создать ясное разделение для естественных и оплаченных результатов поиска. Кроме того, комиссия выпустила извещение для помощи и советов пользователям (рис. 4.8). В настоящее время сервис Google показывает «рекламные ссылки» в правой области страницы результатов поиска (см. рис. 4.1) или выделенными отступом. Сервис Yahoo! показывает оплаченные ссылки под заголовком «sponsor results» в области с особым цветом фона.

Сервис Google находит решение без компромиссов

Пока индустрия поисковых систем решала этические и юридические проблемы, в 2000 году сервис Google нашел свою золотую жилу.

У сервиса уже был алгоритм ранжирования PageRank, результаты которого часто превосходили результаты алгоритмов других поисковых систем. Поиск Google работал быстро, отчасти потому, что инженеры корпорации нашли эффективное решение распараллеливания фоновых процессов и процессов переднего плана, распределив их между несколькими компьютерами. Гигантские хранилища данных корпорации не ощутили бы никакого ущерба, если бы вы вдруг вынули из кластера любой диск. Сервис Google не собирался брать никакой платы за изменение значимости сайтов. Интерфейс сервиса не содержал раздражающих мелькающих баннеров (да и вообще никаких баннеров) ни на странице поиска, ни на страницах результатов. Домашняя страница сервиса представляла собой просто образец аскетизма – почти никаких элементов, кроме слова «Google», строки поиска и кнопок выбора между получением всех результатов (Поиск в Google) или только первого по значимости (Мне повезет!); последняя

опция особенно привлекательна для пользователей с медленным коммутируемым интернет-соединением.

О сервисе Google в 2000 году можно было сказать еще две вещи: во-первых, сервис расширялся, во-вторых, он не приносил больших денег. Технология поиска была превосходной и завоевала доверие множества пользователей. Не было только подходящей бизнес-модели – до появления аукциона Google AdWords.

Уже знакомая по работе сервиса Overture технология позволяла рекламодателям участвовать в аукционах на размещение рекламы на страницах результатов поиска. Но победитель аукциона получал лишь возможность разместить небольшое текстовое рекламное сообщение, с определенным условием, – реклама оставалась рекламой, а не естественным результатом работы поискового алгоритма. Удобство технологии состояло в том, что рекламные ссылки не смешивались с естественными, были относительно ненавязчивыми и, конечно, без назойливых баннеров поперек экрана.

В начале сервис Google взимал плату только за показ рекламы независимо от действий пользователей. В 2002 году технология AdWords была переведена на режим «плата-за-переход», аналогичный нововведению сервиса Overture. Первоначально заказ и оплата рекламных ссылок производились посредством агента корпорации Google. В настоящее время процесс автоматизирован. Чтобы заказать показ рекламы, нужно ввести в веб-форму информацию о ключевых терминах, несколько слов содержания рекламного сообщения и номер кредитной карты для оплаты услуг сервиса Google.

Технологии, объединенные под маркой Google, составили совершенное целое, притом что ни одна из составляющих не была оригинальной.[1] Комбинация решений позволила корпорации стать одним из лидеров рынка. Поскольку рекламная составляющая не оказывала влияния на естественные результаты поиска, его качество осталось на высоте. Сервис AdWords позволил корпорации Google достичь равновесия, которое сами основатели считали недостижимым: коммерческое спонсорство без искажения естественной картины результатов поиска. Корпорации Google удалось набить кошелек, сохранив при этом незыблемыми свои принципы.

Запрещенная реклама

Контекстная реклама, такая как Google AdWords, изменяет рекламную индустрию. Интернет-реклама дает большую отдачу, так как рекламодатель может контролировать целевую аудиторию. Интернет делает возможным показ той или иной рекламы не только по клю-

[1] История развития поискового бизнеса интересно изложена в книге Джона Баттеля (John Battelle) «The Search», Portfolio, 2005.

чевым словам, но и по географическому расположению, чтобы, например, показывать разные ссылки в Калифорнии и Массачусетсе. Успех интернет-рекламы разрушил главный источник дохода многих газет и телеканалов. Средства массовой информации и связи еще не адаптировались к внезапному перераспределению денег и власти.

Успех интернет-рекламы разрушил главный источник дохода многих газет и телеканалов.

Накопив значительные рекламные портфели, поисковые сервисы приобретают способность управлять тем, какие продукты, легально или нелегально, будут продвигаться. Рекламные списки составляются на основе смеси из требований законодательства, рыночных запросов и корпоративной философии. Объединенный эффект представляет собой разновидность «мягкого контроля», давно знакомого газетчикам и приобретающего все большую силу с постепенным превращением поисковых систем в механизмы распространения рекламы. Корпорация Google не принимает рекламные объявления о поддельных дизайнерских товарах, о детской или подростковой порнографии (вообще-то, порнография в США разрешена законом, но только взрослая), о неприемлемых педагогических пособиях, о лекарственных препаратах, которые отпускаются по рецепту, о наркотиках и приспособлениях для их употребления, о фейерверках и пиротехнических устройствах, о сайтах, посвященных азартным онлайн-играм или связанных с ними, о чудодейственных лекарствах, о политических материалах, содержащих обвинения или нападки в отношении частной жизни людей, а также направленных против меньшинств (хотя общеполитическая реклама разрешается), о проституции, об устройствах, связанных с дорожным движением, об определенных видах оружия и др.[1] Разрешаемые материалы фактически составляют то, что рядовые граждане хотят видеть, вправе видеть или стерпят, – и показывают, что корпорация Google благоразумно ограничивает использование своего либерального сервиса для нелегальных целей.

Поиск – сила

На каждом шаге процесса поиска отдельные люди и организации прилагают серьезные усилия для контроля того, что увидит исследователь, – не только ради своих интересов, но и для удобства людей. Поисковые системы не могут обратиться к коллективам экспертов, решающих, что истинно или ложно, что важно, а что и несущественно. Но существуют мощные экономические и социальные мотивы для представления информации согласно человеческим склонностям. И из того что внутренние механизмы работы поисковых систем скрыты от

[1] Политика размещения рекламы средствами Google AdWords.

взора исследователя, следует, что сами системы подконтрольны еще кому-то.

Выполнение по алгоритму не означает отсутствие ошибок

Поскольку поисковые системы вычисляют релевантность и значимость по заданным алгоритмам, люди часто считают, что поисковые системы не подвержены ошибкам. Однако ошибки могут содержаться в самом алгоритме, в неверных весовых коэффициентах различных условий или в механизме получения страниц. Даже само *понятие ошибки* в данной области является весьма субъективным.[1]

Большие деньги не помогут вам купить высокое значение PageRank в системе Google. Алгоритм PageRank не содержит ничего, что могло бы выдвинуть на передний план и без того богатые и влиятельные структуры. Если ваш бизнес процветает, то владельцы многих сайтов сами разместят на своих страницах ссылки на ваш сайт. Это увеличит вашу значимость в поисковой системе, повысит значение PageRank вашего сайта и сделает ваш сайт более популярным усилиями других. Но понятие того, что является настоящей силой и порождает еще большую силу, различается у акул бизнеса и тех, кто едва держится на плаву. Является ли результат поиска «правильным» или настройки алгоритма следует скорректировать – это может определить только человек.

Время от времени некоторые пользователи интернет-магазина Amazon вместо результатов поиска книг по ключевому слову «abortion» (аборт) получали неожиданные результаты, озаглавленные вопросом «Вы, вероятно, имели в виду „усыновление“ (adoption)?». На жалобы администрация магазина отвечала, что результат был автоматически сформирован поисковым алгоритмом из-за схожести слов. Кроме того, журнал работы поисковой системы показал, что клиенты, искавшие книги по первому ключевому слову, часто отправляли запрос и по второму. В конце концов, администрация Amazon приняла *частное* решение трактовать эти слова как абсолютно различные. Таким образом, администрация невольно признала, что поисковый алгоритм содержит возможности ручной настройки – человеческий фактор.[2]

Силы, формирующие рынок, предпочитают, чтобы коммерческие поисковые системы действовали в интересах меньшинства, обладающего политической или иной властью. Владельцы поисковых систем предпочитают идти в ногу со временем и не полагаться на, возможно, бо-

---

[1] Эрик Голдман (Eric Goldman) «Search Engine Bias and the Demise of Search Engine Utopianism» (Разброс результатов поиска и гибель утопии идеальной поисковой системы), *Yale Journal of Law & Technology*, 2005–2006, *http://ssrn.com/abstract=893892*.

[2] Лори Дж. Флинн (Laurie J. Flynn) «Amazon says technology, not ideology, skewed results» (Amazon списывает ошибки результатов поиска на технологию, а не на политику компании), *New York Times* от 20 марта 2006 года.

лее глубокие источники, чтобы удовлетворять спрос пользователей на свежую информацию. Запомните: если вы полагаетесь на результаты поисковой системы при исследовании новой информации, то за компьютерной программой всегда стоит кто-то еще, принимающий окончательные решения о том, что именно вам следует показать.

Поисковые системы не одинаковы

Обращаясь к поисковой системе, вы, вероятно, полагаете, что в результате получите представительную выборку того, что в настоящий момент имеется в Интернете. Следовательно, результаты всех поисковых систем при обработке одного и того же запроса должны быть одинаковыми. Это представление весьма далеко от реальности.

Сравнительное исследование запросов к поисковым системам Google, Yahoo!, Ask и MSN показало, что в 88% случаев результаты на первой странице были совершенно различными. Только в 12% случаев результаты были схожи у двух из четырех поисковых систем.[1] Если вы сильно привязаны к одной системе, то ваш круг поисков существенно ограничен. На сайте *ranking.thumbshots.com* вы можете получить четкое и наглядное представление о степени совпадений результатов различных поисковых систем или различных запросов к одной системе. На рис. 4.9 видно, как мало схожи результаты поиска по запросу «boston florist» (бостонский цветочник) у систем Yahoo! и Google.

Каждая из 100 точек в верхнем ряду представляет собой результат поиска в системе Google, слева направо по мере понижения значимости. Результаты алгоритма Yahoo! расположены в нижнем ряду. Совпадающие ссылки соединены отрезками: в данном случае всего 11 из 100. Первый результат работы системы Yahoo! – поставщик Boston Rose Florist – не появился ни в первой сотне ссылок, ни даже на тридцати первых страницах конкурента.

Значимость веб-страницы определяет ее видимость. Масштабное исследование показало, что 62% пользователей переходят по ссылкам с первой страницы результатов поиска, а 90% – по ссылкам с первых трех страниц. Если пользователи не находят нужной информации, то более 80% из них переформулируют запрос и направят его к той же поисковой системе, надеясь на то, что ответ ей известен, просто вопрос

[1] «Different Engines, Different Results» (Разные поисковые системы – разные результаты), исследование Dogpile.com совместно с Технологическим университетом Квинсленда и Пенсильванским университетом, 2007. Компания Dogpile.com предлагает сервис Metasearch, поэтому результаты исследования могут иметь практическую пользу для компании. Чтобы избежать обвинений в предвзятости, отчет по результатам исследования также содержит полное описание методологии, так что независимая сторона может воспроизвести или проверить результаты.

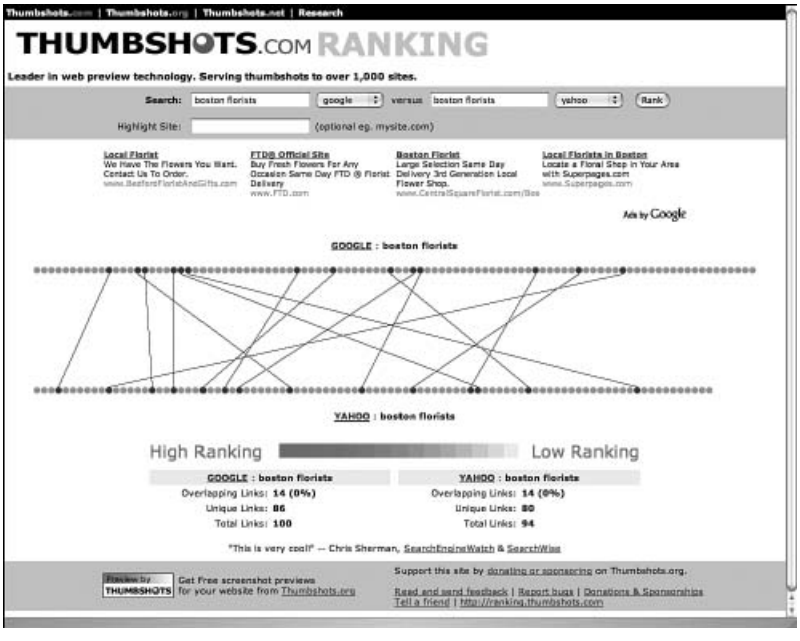


Рис. 4.9. *Сравнение результатов поиска по запросу «boston florist» у систем Yahoo! и Google*

Перепечатка с разрешения корпорации SmartDevil

был поставлен некорректно.[1] Анализ статистики запросов к поисковой системе Excite показал, что более 90% запросов дали удовлетворяющий пользователей результат на первых трех страницах.[2] Анализ статистики системы Google показал, что большинству пользователей достаточно первой страницы.[3]

Значительное число пользователей пребывает в уверенности, что результаты работы поисковых систем не только полезны, но и авторитетны. 36% пользователей считают, что компании с наибольшей значимостью для поисковой системы также являются лидерами в своих областях; только 25% сообщили, что для них высокий рейтинг поис-

---

[1] Исследование iProspect поведения пользователей поисковых систем, апрель 2006 года, *www.iprospect.com/premiumPDFs/WhitePaper_2006_SearchEngineUserBehavior.pdf*.

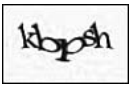
[2] Б. Дж. Йенсен, А. Спинк, Т. Сарацевич (B. J. Jansen, A. Spink, T. Saracevic) «Real life, real users, and real needs: A study and analysis of user queries on the web» (Реальная жизнь, реальные пользователи и реальные потребности: исследование и анализ пользовательских запросов в Сети), *Information Processing & Management*, 36(2), с. 207–227.

[3] Из личной корреспонденции Хэла Абельсона.

кового алгоритма не означает ведущего положения компании.[1] Нет ни одной веской причины считать, что поисковый рейтинг соответствует доле на рынке.

Игра в кошки-мышки со спамерами

Среди сообщений в блогах иногда можно увидеть бессмысленные наборы слов, сопровождающиеся адресом URL. Их оставляет вредоносный бот. Цель «засорения» блога состоит в том, что если паук поисковой системы проиндексирует страницу, то, возможно, сохранит в индексе и адрес. В таком случае значение PageRank сайта, указанного в адресе, возрастет, и сайт поднимется в результатах поиска. Создатели блогов отвечают на это, требуя от пользователя ввести некоторый текст, чтобы иметь возможность оставить сообщение. Этот текст называется «captcha» (от англ. Completely Automated Public Turing test to tell Computers and Humans Apart – полностью автоматизированный публичный тест Тьюринга для различия компьютеров и людей). Эта мера должна помочь определить, что сообщение действительно оставлено человеком, а не ботом. Спамеры могут обойти текст captcha, показывая его добровольным помощникам, а затем автоматизируя процесс ввода. Помощники получают вознаграждение, например бесплатный доступ к порносайтам. Пример изображения captcha:



Сергей Круглов разработал это изображение для Википедии. Применяется во всем мире.

Выводом результатов поиска можно управлять

Сервис веб-поиска – это серьезный бизнес. Большинство пользователей Интернета доверяют результатам работы коммерческих поисковых систем. Покупатели, как правило, переходят по ссылкам на первой странице, хотя состав страницы зависит от сложных и понятных лишь избранным технических деталей работы поискового алгоритма и отличается от сервиса к сервису. Для многих студентов библиотека как источник информации стоит на последнем месте. Они выполняют задания, опираясь на Интернет, и ищут сведения в поисковых систе-

[1] Исследование iProspect, с. 4.

мах. Если поиск проходит неудачно, человек скорее подумает, что некорректно составил запрос, чем попробует другой поисковый сервис, – даже если получает странные и бессмысленные результаты (любой, кто воспользуется поиском Google по запросу «kinderstart» в надежде обнаружить сайт *kinderstart.com*, поймет нас).

В этих условиях каждый, кто собирается заявить о своем веб-сайте всему миру, может прийти к очевидным выводам: во-первых, высокий рейтинг в индексе поисковой системы – это слишком важная вещь, чтобы полагаться здесь на волю случая; во-вторых, поскольку алгоритм поиска – это строгий набор правил, для появления сайта в верхних строчках необходимо при его разработке следовать этим правилам. На втором выводе основана целая индустрия поисковой оптимизации (Search Engine Optimization industry, SEO).

Поисковая оптимизация – это деятельность, направленная на повышение значимости веб-страниц и увеличение их посещаемости. Законопослушные предприниматели оптимизируют свои сайты, чтобы обогнать конкурентов. Мошенники и владельцы порносайтов тоже пытаются обмануть поисковые алгоритмы, маскируясь под добропорядочных участников. Разработчики поисковых систем непрерывно совершенствуют алгоритмы, чтобы отсеять недобросовестные сайты, иногда при этом делая невидимыми и порядочные. Методы усовершенствования держатся в секрете, чтобы избежать контрмер со стороны владельцев вредоносных ресурсов. В этом нескончаемом хаотическом противостоянии немало невинных жертв, которые надеялись на высокие поисковые рейтинги, но оказались ни с чем из-за внезапной смены правил работы поисковых алгоритмов.

Корпорация Google сообщает о своем алгоритме PageRank, что «демократия в Интернете есть»[1], сравнивая накопление поискового рейтинга с народными выборами. Но это довольно слабая аналогия: есть множество хитрых приемов для манипуляции «голосованием», а правила «выборов» довольно туманны.

Ключ к поисковой оптимизации – понимание принципов оценки значимости и формирования рейтинга алгоритмом поиска (какие факторы учитываются, каково их влияние) и применение этих принципов к процессу разработки или адаптации вашего сайта. К примеру, если поисковый алгоритм придает большое значение ключевым словам в заголовке веб-страницы, а вы хотите увеличить рейтинг сайта по запросу «фотокамера», то вам нужно поместить это слово в заголовок. Учитываемые факторы могут быть комплексными и даже внешними по отношению к сайту: внешние ссылки на ваши страницы, возраст ссылок, репутация внешнего сайта. Необходимо потратить много времени, средств и усилий, чтобы занять сколько-нибудь значительную позицию в списке результатов поиска.

---

[1] *http://www.google.com/intl/en/corporate/tenthings.html*

Есть и нечистоплотные приемы. Допустим, вы веб-дизайнер и разрабатываете сайт для Хэла Абельсона. Это будет онлайн-магазин, владелец которого собирается конкурировать с модным универмагом Bloomingdale's. Как привлечь людей на ваш сайт, если они собираются открыть сайт Bloomingdale's? Можно поместить в текст веб-страницы предложение типа «Мы лучше Bloomingdale's». Тогда сайт мистера Абельсона имеет шанс появиться в результатах поиска по запросу «Bloomingdale's». Возможно, вам не хочется афишировать факт конкуренции. Тогда нужно замаскировать ключевое предложение, например, написав его *белым шрифтом на белом фоне*. Человек не увидит текст фразы, потому что смотрит на видимое изображение; индексирующая программа, наоборот, имеет дело с исходным текстом страницы (HTML-кодом), поэтому способ отображения на работу программы не влияет. Если программа не разработана с учетом распознавания подобных «шуток», то дело можно считать сделанным.

Вокруг поисковой оптимизации выросла целая отрасль, наподобие повсеместных курсов подготовки старшеклассников к поступлению в вузы. Поиск в системе Google по ключевой фразе «search engine optimization» возвращает 11 рекламных ссылок, в том числе на сайты, которые дают «гарантию появления на первой странице» и призывают «получить высокий поисковый рейтинг уже сегодня».

Является ли более честной ситуация, когда улучшение поисковых рейтингов за деньги является непрямым, то есть владельцы сайтов обращаются не к поисковым сервисам, а к оптимизаторам? В конце концов, естественно, что если вам есть что сказать миру, то надо сделать это наилучшим образом. А если у вас нет сайта, то, возможно, вам и заявить нечего. Поисковые компании обычно советуют веб-разработчикам просто добросовестно выполнять свою работу, создавая адекватные веб-страницы; аналогично, представители приемных комиссий советуют старшеклассникам просто лучше учиться в школе. Но вряд ли индустрия оптимизации послушается советов и тихо уйдет со сцены.

И что лучше – для общества в целом, а не для поисковых сервисов или компаний, опирающихся на их услуги, – трудно сказать. В книге «Ambient Findability» (O'Reilly, 2005)[1] Питер Морвиль (Peter Morville) описывает усилия по поисковой оптимизации сайта *www.cancer.gov* Национального института рака США (U. S. National Cancer Institute).

Цель создания сайта состояла в том, чтобы обеспечить достоверной и актуальной информацией тех, кто более всего в ней нуждался, – преимущественно больных раком и членов их семей. Поиск по ключевому слову «cancer» (рак) давал удовлетворительные результаты. Однако этого было недостаточно, потому что большинство пользователей осуществляли поиск по специфическим формам заболевания.

[1] Питер Морвиль «Тотальная видимость. Как наши находки меняют нас». – Пер. с англ. – СПб.: Символ-Плюс, 2008.

Институт привлек к работе специалистов по оптимизации, и в настоящее время тот, кто ищет, например, «colon cancer» (рак толстой кишки) в одной из верхних строчек получает ссылку на соответствующий раздел сайта.

Хорошо ли это? Возможно. Если не верить Национальному институту рака, то кому вообще можно верить? Однако источник медицинской информации WebMD (*www.webmd.com*) и другие коммерческие сайты, сражающиеся за верхние строки страниц результатов поиска, могут не согласиться с этим мнением. А объединение Национальный круглый стол по проблемам лечения колоректальной формы рака (National Colorectal Cancer Roundtable) вообще не поднимается выше седьмой страницы – слишком глубоко, чтобы быть замеченным подавляющим большинством пользователей.

«Бомбардировка Google»

«Бомба Google» – это трюк, вызывающий реакцию поисковой системы в виде совершенно неадекватных запросу результатов (часто с политическим подтекстом). К примеру, если вы запускали поиск по запросу «miserable failure» (позорный провал) после выборов президента США 2000 года, то могли попасть на сайт Белого дома в раздел биографии Джорджа Буша. Одна из организаций по борьбе за свободу личности Liberty Round Table предприняла усилия в том числе против Центра работы науки в интересах общества (Center for Science in the Public Interest, CSPI). В начале 2008 года на сайте *www.libertyroundtable.org* можно было прочесть: «Вы еще не вкусили прелесть «бомб Google»? Обратите оружие смеха против недобросовестных производителей пищевой продукции и организованной преступности. Ваше участие может реально изменить расстановку сил. Прочтите, что нужно сделать, и присоединяйтесь к веселью! Текущая цель – оператор Verizon Communications, ограничение гражданских прав». Далее было написано, какой HTML-код нужно было включить в текст своей веб-страницы, чтобы повлиять на работу алгоритма Google.

Марек В., двадцатитрехлетний программист из Цешина (Польша) подверг «бомбардировке Google» президента страны Леха Качиньского. Поиск по слову «kutas» (пенис) возвращал в верхней строке ссылку на президентский веб-сайт. Помимо того что г-ну Качиньскому такая шутка совершенно не понравилась, оскорбление президента в Польше считается преступлением. Теперь Мареку предстоит отбыть 3 года в тюрьме.[1]

[1] *blogoscoped.com/archive/2007-09-11-n78.html*

Борьба за оптимизацию – это вечная игра в кошки-мышки. Оптимизаторы ищут новые способы повышения значимости; разработчики поисковых систем проектируют алгоритмы, обеспечивающие максимальную релевантность результатов поиска. В этой игре страдают и посторонние. Бизнес Нила Монкрифа, владельца онлайн-магазина обуви больших размеров, какое-то время процветал, поскольку поиск по запросу «big feet» (большие ноги) выводил ссылку на сайт магазина *2bigfeet.com* первым номером. В один прекрасный день сервис Google в борьбе с недобросовестными оптимизаторами изменил поисковый алгоритм, и ни в чем не повинный сайт мистера Монкрифа оказался на 25 странице, что обернулось для его веб-ориентированного и малодоходного бизнеса катастрофой.[1]

Манипулирование поисковыми рейтингами происходит на поле, где грубая сила не имеет значения. Поскольку веб-поиск является точкой входа во вселенную информации Всемирной паутины, управление поиском может влиять даже на мышление людей. В это управление вовлечены даже правительства.

Поисковые системы не могут видеть всего

Обычные поисковые системы пропускают огромное количество информации, доступной в Интернете. Пауки не могут сканировать базы данных, читать форматы документов, такие как PDF, или исследовать содержимое сайтов, требующих элементарной регистрации. Приложив немного больше усилий, чем ввод нескольких слов в строке поиска, вы можете найти действительно то, что вам нужно. Серьезной ошибкой будет считать, что информация является незначительной или не существует только потому, что ее нет в индексе поисковой системы. Хороший обзор ресурсов для поиска нужной информации в лабиринтах Всемирной паутины можно найти на сайте Роберта Лэки *www.robertlackie.com*.

Контроль поиска и контроль умов

Чтобы сделать библиотечную книгу недоступной читателю, не нужно убирать ее с полки. Достаточно удалить соответствующую запись из библиотечного каталога: нет записи – нет книги.

Ища информацию в Интернете, люди порой необоснованно полагают, что поисковый индекс является полным отражением существующего информационного поля. Поисковые системы подобны биноклю, помогающему разглядеть на цифровом ландшафте интересующие нас детали.

Исчезновение документов в цифровом мире не всегда означает их стирание – возможно, документы просто выпали из поля зрения поисковой системы.

[1] Джон Баттель (John Battelle) «The Search», глава 7.

В то же время окуляры бинокля не могут охватить весь ландшафт. Подобно библиотечной книге информация, которую нельзя найти, все равно что не существует. Исчезновение документов в цифровом мире не всегда означает их стирание – возможно, документы просто выпали из поля зрения поисковой системы.

Путем контроля «находимости» можно как скрывать информацию, так и, наоборот, выставлять ее напоказ. Средства поиска стали орудием в руках правительств, стремящихся ограничить общение граждан своих стран с окружающим миром (к этой теме мы еще вернемся в главе 7). Когда Интернет пришел в Китай, в Поднебесную хлынул поток прежде недоступной информации. Правительство отреагировало созданием «Великой китайской информационной стены», блокирующей нежелательную информацию. Но биты прибывали быстрее, чем им успевали преграждать пути. На Съезде компартии Китая в 2002 году была принята простая контрмера – блокирование поисковых систем. «В Интернете много вредной информации, – заявил китайский представитель. – Нельзя допускать всех к вредной информации». В частности, была блокирована система Google из-за функции предоставления пользователям кэшированных страниц.[1]

Поиск в Интернете уже стал настолько важен для китайской экономики, что нельзя было пускать работу «Великого фильтра» на самотек. «Строители» старались, совершенствуя свое творение. Однако ссылки на блокированные сайты иногда появлялись в результатах поиска. На сайт нельзя было перейти, но, по крайней мере, можно было узнать, что от вас скрывают.

В 2004 году под угрозой отключения на территории Китая корпорация Google согласилась подвергнуть цензуре свою службу новостей, предоставляющую доступ к онлайн-изданиям средств массовой информации. Корпорация нехотя согласилась не предоставлять никакой информации, так как «простой показ заголовков может привести к тому, что на территории Китая служба Google News будет блокирована».[2] Однако правительство еще не было готово.

Черные дни настали год спустя. Поскольку серверы корпорации Google были расположены за границами Китая, сервис поиска был доступен, но отклики приходили очень медленно. Кроме того, большинство возвращаемых ссылок были бесполезны. Сервис Google оказался не у дел, а большую часть бизнеса захватил китайский поисковый сервис Baidu.

---

[1] «China blocking Google» (Китай блокирует Google), *BBC News* от 2 сентября 2002 года, *news.bbc.co.uk/2/hi/technology/2231101.stm*; «Google fights Chinese ban» (Google борется с китайскими запретами), *BBC News* от 3 сентября 2002 года, *news.bbc.co.uk/1/hi/technology/2233229.stm*.

[2] Блог Google, 27 сентября 2004 года, *googleblog.blogspot.com/2004 года./09/china-google-news-and-source-inclusion.html*.

Корпорация Google встала перед суровым выбором: поддаться политике интернет-цензуры китайского правительства или потерять китайский сегмент рынка. Как соблюсти баланс между обязательствами перед пайщиками и корпоративной миссией – «организовать мировую информацию и сделать ее всесторонне доступной и полезной»?[1] Сможет ли компания, основанная выходцем из Советского Союза, мирно сотрудничать с китайской коммунистической цензурой?

«Всесторонняя доступность» недостижима для корпорации Google даже в США. Если правообладатель заявит, что корпорация, предоставляя всеобщий доступ к частным материалам, нарушает его права, ссылка на материалы должна быть немедленно убрана. Кроме законов, защищающих авторские права, есть и другие, например Акт о пристойности в коммуникационных сетях (Communications Decency Act), обсуждаемый в главе 7.

Сервис Google в США и в Китае

Проверьте сами:

- в США доступна версия *www.google.com*
- в Китае доступна версия *www.google.cn*

Приспосабливание корпорации к китайскому праву было, по сути, ничем иным, как нормальной практикой любой компании: следует уважать законы той местности, где вы ведете бизнес. Китай отразил американскую критику относительно строгости законов. «После изучения интернет-законодательства США мы обнаружили, что базовые принципы наших правовых целей и принципов совпадают, – сообщил Лю Чжэнжун, вице-президент Бюро по делам Интернета при Государственном совете по информации Китайской народной республики. – Это несправедливо и попахивает двойными стандартами, когда <иностранные державы> критикуют Китай за удаление противозаконных или вредоносных сообщений, в то время как в США эти действия вполне законны».[2]

В итоге, когда корпорация Google согласилась подвергнуть цензуре китайскую ветвь своего сервиса, некоторые пробудились от своих мечтаний о глобальной информационной утопии. «Ограничение результатов поиска несовместимо с миссией корпорации Google, однако полное лишение пользователей информации (или представление совершенно искажен-

---

[1] *www.google.com/corporate/*; *www.google.com/corporate/*

[2] Питер Поллак (Peter Pollack) «Congress grills tech firms over China dealings» (Конгресс устраивает взбучку технологическим компаниям, пошедшим на поводу у китайских властей), *Arstechnica* от 15 февраля 2006 года, *arstechnica.com/news.ars/post/20060215-6192.html*.

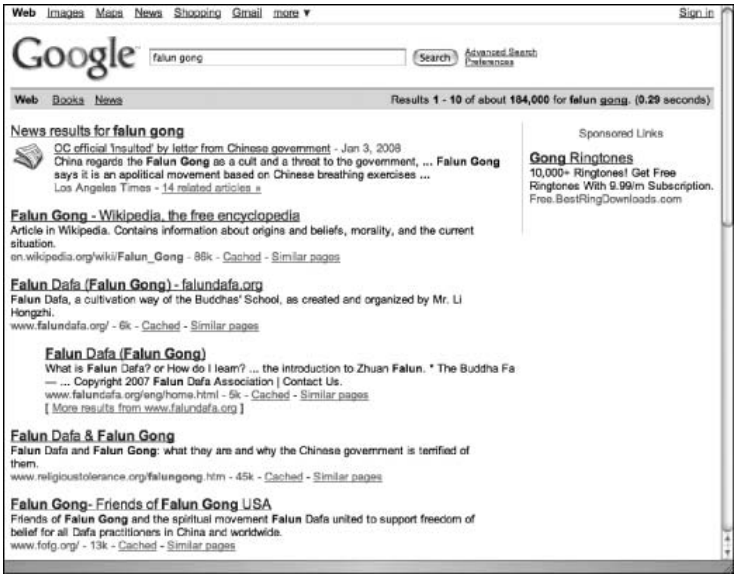


Рис. 4.10. *Результаты поиска по запросу «**falun gong**» **в американской** версии сервиса **Google***

*Google™ **является зарегистрированной торговой маркой. Перепечатка** с разрешения корпорации **Google***

ной и, следовательно, бесполезной) еще менее соответствует нашей политике», – говорилось в официальном заключении.[1] Некоторым это заявление показалось малодушным. Один разочарованный борец за права заявил: «Зло существует в мире только с вашего позволения».[2] (Явный намек на другой принцип корпорации: «Не причиняй зла». Теперь этот принцип пересмотрен и выглядит так: «Можно заработать, не причиняя зла».) Конгресс США вызвал поисковые компании (Google в том числе) на слушания. «Ваши отвратительные действия в Китае позорны, – заявил представитель от штата Калифорния Том Лантос. – Я не понимаю, как ваше руководство может спокойно спать по ночам».[3]

---

1 Кевин Дж. Дилэйни (Kevin J. Delaney) «Google launches service in China» (Google открывает свой сервис в Китае), *Wall Street Journal* от 25 января 2006 года.

2 Памела Геллер Ошри (Pamela Geller Oshry), цитируется Гайаватой Брэем (Hiawatha Bray) в «Google China censorship fuels calls for U.S. boycott» (Цензура Google в Китае бойкотируется в США), *Boston Globe* от 28 января 2006 года.

3 Верн Копытофф (Verne Kopytoff) «Lawmakers bash top high-tech firms for yielding to China» (Законодатели наказывают ведущие высокотехнологичные компании за работу в Китае), *San Francisco Chronicle* от 16 февраля 2006 года.

Рис. 4.11. *Результаты поиска по запросу «**falun gong**» в китайской версии сервиса **Google** (**Google China**)*

Google™ является зарегистрированной торговой маркой. Перепечатка с разрешения корпорации Google

Результаты унизительного компромисса корпорации Google шокируют, в чем может убедиться каждый. На рис. 4.10 показаны верхние результаты поиска в американской версии по запросу «falun gong» (фалуньгун).

Для сравнения на рис. 4.11 показаны результаты поиска по тому же запросу в китайской версии сервиса. Все результаты указывают на источники явно негативного отношения к религиозному движению Фалуньгун или отчеты о предпринятых против него правительственных мерах.

Большая часть поиска по американской или китайской версии сервиса Google дает одинаковые результаты. Например, если вы ищете «обувь», то получите рекламные ссылки на обувные онлайн-магазины, так что сервис может оплатить свои затраты.

Но есть и немало исключений. Один исследователь протестировал китайскую версию сервиса Google на 10 тысячах слов и обнаружил, что цензуре подверглось результатов приблизительно 9%.[1] Существовали различные комбинации ключевых слов, и они нередко менялись. Среди вариантов были «преступление против человечества», «угнетение» и «геноцид», а также списки диссидентов и политиков.

Окуляры поисковой системы не являются кристально чистыми. То, что вы видите, определяет ваше мышление. Представитель корпорации Google ответил Конгрессу: «В несовершенном мире нам приходится делать несовершенный выбор», – и это чистая правда. Но бизнес есть бизнес. Как заметил генеральный директор корпорации Эрик Шмидт о ее деятельности, «есть множество способов управлять миром и своей компанией... Если вам это не нравится, *не участвуйте*. Вы здесь находитесь совершенно добровольно; силком вас сюда не затаскивали».[2]

На веб-сайте проекта OpenNet Initiative Центра Беркмана по изучению Интернета и общества *opennet.net* находится сервис, позволяющий узнать, в каких странах заблокирован доступ к тем или иным сайтам. Сводка результатов опубликована в виде книги под названием «Access Denied» (Запрещенный доступ), MIT Press, 2008.

ЧТО вы искали? Отслеживание поисковых запросов

Поисковые системы могут хранить всю историю ваших поисковых запросов и ссылок, по которым вы переходите. В мире носителей практически неограниченной емкости поисковым компаниям выгодно хранить эти данные: они могут однажды пригодиться и являются важным элементом процесса поиска. При этом возникают правовые и этические вопросы. Возможность накапливать и анализировать историю запросов дает источник власти. Власть исходит из знания о ваших интересах как личности и об интересах общества в целом.

Но зачем владельцам поисковых сервисов хранить историю запросов и переходов по ссылкам? Есть важные причины, по которым людям хотелось бы избежать этого: неприкосновенность частной жизни подвергается опасности, когда подобные данные накапливаются, как уже обсуждалось в главе 2. К примеру, согласно Патриотическому акту федеральное правительство при определенных обстоятельствах

[1] *blogoscoped.com/archive/2006-06-18-n85.html.*

[2] Джон Баттель (John Battelle) «The Search», с. 228.

может запросить журнал ваших действий у поисковой компании, даже не уведомляя вас об этом. Это еще легче представить в странах с более жесткими режимами. Китайские диссиденты были отправлены в тюрьму после того, как правительство получило от компании Yahoo! (в соответствии с местными законами!) их электронную почту.[1] Член Палаты представителей Крис Смит задал вопрос: «Если бы полвека назад гестапо запросило сведения о местонахождении Анны Франк, правильно ли было бы передать тайной полиции эти сведения согласно местному законодательству?» А если данные представляют собой не электронную почту, а журнал поисковых запросов? С точки зрения самих поисковых компаний причина сохранения истории запросов проста. Сооснователь корпорации Google Сергей Брин раскрыл эту причину на веб-странице «Философия» корпорации: «Идеальная поисковая система точно определит, что подразумевает пользователь, и покажет именно те результаты, которые ему нужны». Ваша история запросов накапливается, и Джен сможет понимать вас лучше, зная, о чем вы думали в прошлом.

Поиск изображений

В Интернете есть сервисы, предназначенные для поиска изображений. Поиск по лицам создает еще одну угрозу неприкосновенности частной жизни. Некоторое время назад технологии компьютерного распознавания лиц стали достаточно быстрыми и надежными. Компьютеры справляются с поиском одинаковых лиц на изображениях лучше, чем люди. Сегодня в Интернете общедоступны миллионы фотографий, и чтобы найти на них ваше лицо, нужна всего одна ваша фотография. Похожая технология позволяет искать онлайн товары с помощью похожих изображений. Примеры общедоступных сервисов сравнения изображений: *riya.com*, *polarrose.com* и *like.com*.[2]

Качество поиска может повыситься, если анализировать предыдущие данные о запросах. Ради сохранения личной неприкосновенности можно заставить поисковую систему забыть историю, но этому есть своя цена. При отказе от истории запросов можно получить менее адек-

---

[1] Ариана Юньчжун Ча и Сэм Диаз (Ariana Eunjung Cha, Sam Diaz) «Advocates sue Yahoo in Chinese torture case» (Адвокаты возбуждают дело против Yahoo в Китае), *Washington Post* от 19 апреля 2007 года.

[2] Рэй Блитштейн (Ray Blitstein) «Image analysis changing way we search, shop, share photos» (Анализ изображений изменяет способы, которыми мы ищем, покупаем, делимся фотографиями), *San Jose Mercury News* от 30 апреля 2007 года.

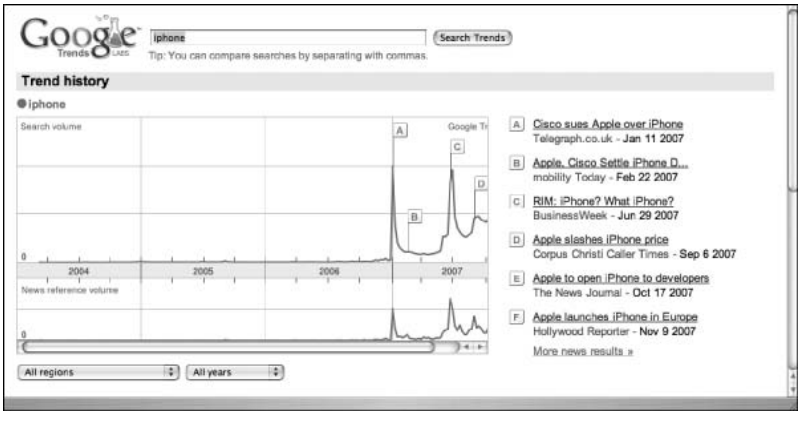


Рис. 4.12. *Верхняя линия показывает количество запросов к системе* ***Google*** *по слову «iPhone», а нижняя – количество упоминаний о мобильном телефоне* ***Apple iPhone в индексированных новостных статьях***

Google™ является зарегистрированной торговой маркой. Перепечатка с разрешения корпорации Google.

ватные результаты; для поисковой системы это означает снижение конкурентоспособности. В очередной раз убедившись, что бесплатный сыр бывает только в мышеловке, люди спустя некоторое время перестают беспокоиться о персональной истории запросов и оставляют все как есть.

Даже без привязки к отдельным людям накопленная общая история запросов спустя некоторое время начинает представлять интерес для маркетингового и экономического анализа. На рис. 4.12 показан тренд поиска в системе Google по запросу «iPhone» совместно со ссылками на определенные ключевые новостные статьи, касающиеся мобильного телефона Apple iPhone. Сервис поиска создал новый вид капитала – миллиарды битов информации о том, что люди хотят знать.

Поищите тренды на странице *www.google.com/trends*.

Контроль и замена посредников

Поисковые системы стали ключевыми фигурами в управлении тем самым цифровым миром, который некогда был задуман как утопичная децентрализованная вселенная свободно движущейся информации.

Важная часть истории поиска в Интернете – не о технологии или прибылях, хотя есть немало и того, и другого. Эта часть истории – о власти, власти делать вещи видимыми, вызывать их к существованию или отправлять в небытие, контролировать информацию и доступ к ней.

Поисковые системы стали ключевыми фигурами в управлении тем самым цифровым миром, который некогда был задуман как утопичная децентрализованная вселенная свободно движущейся информации.

Поисковые системы приобретают коммерческую ценность не путем создания информации, но путем помощи людям в ее поиске, понимания их потребностей и организации соответствующей контекстной рекламы. Некоторые критики несправедливо обозначают эту деятельность термином «эксплуатация», поскольку сами не могут создать чего-то более творческого (см. главу 6). Это поразительный феномен: *предоставление доступа к информации имеет большую коммерческую ценность, чем создание информации.* Рыночная капитализация корпорации Google (157 млрд долларов) на 50% превышает объединенную капитализацию газеты *New York Times* (3 млрд долларов), издательства Pearson Publishing (13 млрд долларов), аукциона eBay (45 млрд долларов) и торговой сети Macy's (15 млрд долларов). Компания, предоставляющая доступ к данным, к созданию которых не имеет никакого отношения, имеет бóльшую рыночную ценность, чем создатели данных. На базаре битов львиная доля достается не лавочникам, а посредникам.

Накопление и перераспределение власти – неожиданный побочный эффект поисковой индустрии. Следует ли сконцентрировать контроль над ней в определенных руках, или контроль должен быть доступен каждому (а не только сервисам вроде Search Engine Watch, сайт *searchenginewatch.com*)? Высказывались предложения вроде принудительного опубликования алгоритмов поиска и ранжирования, но пока существует конкуренция, реализация таких предложений не встречает широкой поддержки. А конкуренция есть – хотя корпорация Microsoft и обращалась в Федеральную торговую комиссию с заявлением, что сервис Google собирается «контролировать виртуальную монополию» интернет-рекламы.[1] Это заявление (кстати, отвергнутое комиссией) немало позабавило тех, кто вспомнил яростное сопротивление самой корпорации Microsoft обвинениям в монополизации рынка настольного программного обеспечения еще несколько лет назад. В цифровом мире все меняется быстро.

[1] «Summary of Antitrust Analysis: Google's Proposed Acquisition of DoubleClick» (Итоги антимонопольного анализа: предполагаемый сбор двойных щелчков Google), меморандум Microsoft, доступный на Google Watch, 24 декабря 2007 года, *googlewatch.eweek.com/content/google_vs_microsoft/meet_google_search_giant_monopolist_extraordinaire.html.*

Открытые альтернативы

Есть сотни поисковых проектов, созданных как программное обеспечение с открытым исходным кодом. Каждый может получить исходный код проектов и исследовать механизмы его работы. Большинство альтернативных проектов не индексируют весь Интернет – это слишком обширная область. Проект Nutch (*lucene.apache.org/nutch*, *wiki.apache.org/nutch*) пока еще находится в стадии разработки, но уже используется в различных областях. Развивающийся проект Wikia Search основателя интернет-энциклопедии Википедия Джимми Уэйлса (*search.wikia.com/wiki/Search_Wikia*) использует программное ядро Nutch и основывается на пожеланиях сообщества по развитию технологии поиска. Прежде всего, базовым принципом провозглашается отсутствие любых возможных утечек персональной информации.

Метапоиск

Сервисы вроде *copernic.com*, *surfwax.com* и *dogpile.com* являются своеобразными надстройками над существующими поисковыми системами (сервисами метапоиска) – они переадресуют ваши запросы к нескольким реальным поисковым системам и на основе своих критериев покажут обобщенные результаты. Согласно эксплуататорской теории интернет-поиска сервисы метапоиска эксплуатируют эксплуататоров!

Так что в настоящее время сервисом поиска правят законы рынка, и покупатели должны быть начеку. Возможно, так и должно быть. Слишком часто кажущиеся благими усилия по управлению технологиями причиняли больший вред, чем предполагаемое зло, против которого эти усилия были направлены. Мы еще увидим примеры этого в следующих главах.

Мы привыкли рассчитывать на поисковые системы. Но мы не знаем, как они работают, и у нас нет простых ответов, как на это реагировать. Президент Франции Жак Ширак ужасался тому, что весь мир мог бы полагаться на американские системы как на информационных посредников. Чтобы противостоять американской гегемонии, Франция и Германия в 2006 году анонсировали план разработки поисковой системы, финансируемой государством. Президент Ширак заявил: «Мы должны достойно ответить на вызов, брошенный американскими гигантами Yahoo! и Google. Для этого мы запустим европейскую поисковую сис-

тему Quaero».[1] Как объяснил глава Франции, европейские правительства примут участие в этой ранее приватной индустрии «под впечатлением потрясающего успеха Airbus... Культура не является объектом продажи и не может быть отдана во власть слепых стихий рынка». Годом позже Германия вышла из проекта, как сообщил некий источник в отрасли, из-за того что «Германии явно надоела вечная французская публичная порка Америки и идея разработки альтернативы Google».[2]

Технологии поиска совместно с информационной емкостью Всемирной паутины вызвали поразительный эффект глобальной доступности разнообразных данных. Негативные стороны, порожденные возможностью ограничивать видимость информации, не могут пересилить потенциал неограниченного познания. Вещи, невообразимые десяток лет назад, сегодня кажутся простыми. Люди могут найти своих родственников. Люди могут общаться с новыми группами поддержки и находить актуальную медицинскую информацию, в том числе малоизвестную. Людям доступны факты из книг, которых они никогда не держали в руках. Средства поиска приоткрывают человечеству просветительскую роль цифровой экспансии и дают возможность увидеть желаемое.

Технологии шифрования созданы с обратной целью: сделать информацию тайной, даже если она распространяется через общедоступные коммуникационные сети. Эта полная парадоксов тема о политике и математике составляет предмет обсуждения следующей главы.

---

[1] Кевин Дж. О'Брайен (Kevin J. O'Brien) «Europeans weigh plan on Google challenge» (Европейцы планируют создать конкурента Google), *International Herald Tribune* от 18 января 2006 года; «Attack of the Eurogoogle» (Атака Eurogoogle), *Economist.com* от 9 марта 2006 года.

[2] Описание проекта поиска изображений и видео Theseus, *Pandia Search Engine News*, 28 ноября 2007 года *http://www.pandia.com/sew/570-theseus.html*.

Глава 5 | Засекреченные биты

Как создаются криптостойкие шифры

Средства шифрования в руках террористов и прочих

13 сентября 2001 года, Нью-Йорк, США. Пламя все еще бушует над обломками Всемирного торгового центра. В это время представитель штата Нью-Хэмпшир Джадд Грег докладывает Сенату о случившемся. Сенатор повторяет предупреждения, сделанные ФБР несколько лет назад: одним из самых серьезных препятствий для работы спецслужб является «возможность обмениваться зашифрованной информацией людям, намеренным принести вред стране». «Мы привыкли, – продолжал сенатор Грег, – что можем взломать большинство шифров с помощью наших средств и интеллекта».[1] И не более того. «Технология превзошла возможности криптоаналитиков».[2] Даже либеральный гражданский специалист по шифрованию Фил Циммерманн, чьи общедоступные программы для шифрования с 1991 года применяли борцы за права человека во всем мире, признал, что террористы в принципе могли шифровать свою переписку. «Я всего лишь допускаю, – заявил Фил Циммерманн, – что некто, планирующий настолько дьявольское действие, мог бы пожелать скрыть свои приготовления с помощью технологий шифрования».[3]

Шифрование (криптография) – это искусство кодирования сообщений, так что они не могут быть прочитаны противником или любителями читать чужие письма. Чтобы расшифровать сообщение, требуется знать последовательности символов – «ключ», которым оно было зашифровано. Зашифрованное сообщение может быть доступно

---

1 Стенограмма заседания Конгресса, 13 сентября 2001 года, с. S9357.

2 Джон Шварц (John Schwartz) «Disputes on electronic messages: Encryption takes on new urgency» (Диспуты по электронным сообщениям: второе рождение шифрования), *New York Times* от 25 сентября 2001 года.

3 Там же.

кому угодно, но без ключа его содержимое так же остается в тайне, как если бы сообщение хранилось в закрытом сейфе. Пока нет ключа – подходящего ключа – сейф (или сообщение) продолжает хранить свою тайну.

Когда требовалось, была и «совместная общественная деятельность, которая спроектировала и реализовала программное обеспечение и построила среду, обеспечивающую существование технологий шифрования», – утверждал сенатор Грег. Эта деятельность регулировалась законодательством. Создатели программ для шифрования должны были предоставить правительству лазейки для обхода защиты и декодирования сообщений. Но программы создавались по всему свету и могли распространиться в мгновение ока, как это произошло с программами Циммерманна. Для создания доступных правительству США «черных ходов» в программах Соединенные Штаты должны были бы использовать «американский рынок как средство» формирования зависимости иностранных поставщиков и вынудить их действовать по американским правилам.

К 27 сентября законодательная инициатива сенатора приобрела четкие формы. Ключи для шифрования сообщений следовало хранить у правительства под строгим секретом. Это будет «квази-правовая сущность», как постановил Верховный суд США, вынесший также решение о случаях, в которых ключи могли бы быть открыты. Борцы за права человека немедленно возмутились и выразили сомнение в том, что идея хранения ключей у третьей стороны вообще может работать. «Это ничего, – парировал сенатор в конце сентября. – Ничто не совершенно. Если мы не попытаемся, то ничего не сможем сделать. Если попытаемся, то приобретем, по крайней мере, фундамент для создания чего-то более совершенного».[1]

Спустя три недели сенатор Грег внезапно приостановил движение своей законодательной инициативы. «Мы не работаем над законопроектом о шифровании и не намерены этого делать», – заявил представитель сенатора 17 октября 2001 года.[2]

24 октября 2001 года Конгресс принял Акт о патриотах, давший ФБР существенно новые возможности в борьбе с терроризмом. Но в Акте нет ни слова о шифровании. После инициативы сенатора Грега власти США не предприняли никаких серьезных попыток законодательно контролировать разработку программного обеспечения для шифрования.

---

[1] Там же.

[2] Деклан МакКалло (Declan McCullagh) «Senator backs off backdoors» (Сенатор ведет скрытые действия), *Wired News* от 17 октября 2001 года.

Почему бы не контролировать шифрование?

В 1990-х ФБР сделало контроль шифрования своим правовым приоритетом. Инициатива сенатора была довольно мягкой формой законопроекта, разработанного ФБР и предложенного к рассмотрению избираемым Комитетом Сената по разведке (United States Senate Select Committee on Intelligence, SSCI) в 1997году.[1] В тексте проекта, в частности, содержалось предложение о заключении в тюрьму сроком на пять лет того, кто продавал программы для шифрования, не обеспечивающие представителями власти возможность немедленного декодирования сообщений.

Как могли меры, представлявшиеся необходимыми для борьбы с терроризмом в 1997 году, выпасть из поля зрения законодателей через четыре года после наиболее разрушительной террористической атаки, когда-либо предпринятой в отношении Соединенных Штатов?

Осенью 2001 года ни в законодательстве о криптографии, ни в соответствующей дипломатии не произошло существенных сдвигов. Никаких других оснований считать применение технологий шифрования террористами или организованной преступностью малозначительной проблемой также не было найдено. Сформировалось лишь еще одно важное явление в сфере практической криптографии – бурный рост числа коммерческих транзакций, совершенных через Интернет. И Конгресс внезапно осознал, что для экономики просто необходимо разрешить банкам и их клиентам, авиалиниям и пассажирам, аукциону eBay и магазину Amazon применять средства шифрования. Каждый, кто совершает коммерческие операции через Интернет, нуждается в криптографических средствах обеспечения безопасности сделки. Многим людям во всем мире стали вдруг понадобились надежные средства шифрования, и от этого зависела вся мировая экономика.

Напряжение между обеспечением надежности коммерческих операций и предотвращением тайной переписки между преступниками ощущалось около десяти лет. Сенатор Грег был одним из последних инициаторов ввода ограничений применения технологий шифрования. Национальный совет США по научным исследованиям (United States National Research Council, NRC) в 1996 году выпустил отчет на 700 страницах, в котором были указаны достоинства и недостатки использования криптографических средств. В заключении отчета указы-

[1] «Тот, кто после 31 января 2000 года будет продавать на внутреннем или внешнем рынке криптографические продукты, не содержащие свойств или функций, позволяющих официально уполномоченным лицам получить немедленный доступ к открытому тексту или расшифровать данные, может быть наказан тюремным заключением на срок до пяти лет с наложением штрафа или без оного», 105-е заседание Палаты представителей Конгресса, отчет 695, 104–108, часть 4 Акта о безопасности и свободе при помощи шифрования 1997 года, раздел 2803.

валось, что попытки контролировать технологии шифрования будут неэффективны и что вред, нанесенный этими действиями, превысит возможные выгоды.[1] Отчет не убедил представителей служб разведки и обороны страны. Директор ФБР Луи Фри, выступая перед Конгрессом в 1997 году, заявил, что «ограничивающее законодательство является выражением нашего общего мнения о том, что широкомасштабное применение криптостойких <не предоставляющих правительству ключ> средств шифрования окончательно сведет к нулю все наши возможности по борьбе с терроризмом и организованной преступностью».[2]

Даже четыре года спустя после атаки 11 сентября для нужд экономики не было предложено ни одной альтернативы повсеместному распространению криптографического программного обеспечения и использованию его на компьютерах коммерческих организаций или граждан, совершающих электронные сделки. В 1997 году рядовые граждане (так же, как и выборные представители власти) не могли что-то купить во время интернет-сеанса. Члены семей конгрессменов едва ли были активными компьютерными пользователями. К 2001 году все это изменилось – цифровая экспансия набрала темп. Компьютер стал обычным потребительским товаром, Интернет вошел в дома американцев – и вместе с ним пришла опасность кражи персональной (в том числе, финансовой) информации. Пользователи не хотели, чтобы их даты рождения, номера кредиток или идентификаторы социального страхования появились в Интернете для всеобщего обозрения.

Почему шифрование настолько важно для интернет-коммуникаций, что Конгресс США позволил себе пренебречь террористической угрозой ради возможности применения технологий шифрования коммерческими организациями и отдельными потребителями? Прежде всего, в необходимости защиты информации нет ничего нового. Те, к примеру, кто отправляет письма в конвертах обычной почтой, достаточно уверены в конфиденциальности безо всякой криптографии.

Ответ связан с открытой архитектурой Интернета. Биты пересылаются по Сети не непрерывным потоком, а отдельными блоками – пакетами. Пакет состоит не больше, чем из 1500 байт (см. приложение). Пакеты данных можно сравнить не с конвертами, где адрес снаружи, а содержимое внутри, а с открытками, где вся информация на виду. По мере перемещения по Интернету пакеты путешествуют от одного промежуточного компьютера к другому. Эти узловые компьютеры называются *маршрутизаторами*. Каждый пакет данных при попадании к маршрутизатору сохраняется, проверяется, анализируется

---

[1] Национальный совет по научным исследованиям, Кеннет У. Дэм и Герберт С. Лин (Kenneth W. Dam, Herbert S. Lin) «Cryptography's Role in Securing the Information Society» (Роль криптографии в обеспечении безопасности информационного общества), National Academy Press, 1996.

[2] Выступление директора ФБР Луи Фри (Louis Freeh) перед сенатскими слушаниями по шифрованию 9 июля 1997 года.

и пересылается ближе к пункту назначения. Для оптоволоконных или медных кабелей можно обеспечить защиту и неприступность, но при пересылке данных по беспроводным каналам биты могут быть считаны из эфира, причем без всякой возможности узнать о факте считывания.

Отправить номер своей кредитки универмагу в простом сообщении электронной почты – примерно то же самое, что выйти на Таймс Сквер и объявить его во всеуслышанье. К 2001 году огромное количество кредитных номеров путешествовало в виде битов по оптволоконным кабелям или в эфире и не было никакой возможности помешать любителям шпионажа считать эти данные.

Способ обеспечения безопасности интернет-коммуникаций – чтобы никто, кроме адресата, не мог прочесть сообщение – заключается в шифровании данных. Только получатель должен иметь возможность декодировать сообщение. В этом случае любители шпионажа могут сколько угодно исследовать пакеты на пути между маршрутизаторами. Все, что получит излишне любопытный пользователь, – это бессмысленный набор битов.

В мире, где началась электронная коммерция, криптография больше не может быть тем, чем она была с античности до начала третьего тысячелетия: оружием, применяемым военачальниками и дипломатами для защиты жизненно важных государственных секретов. Даже в начале 1990-х Государственный департамент США постановил, что исследователь криптографических методов должен был регистрироваться подобно международному торговцу оружием. Нынче криптография гораздо больше похожа на инкассаторский броневик, чем на оружие. Она уже не военное снаряжение, а деньги.

Создание потребительской ценности этого прежде военного средства уже не просто технологический сдвиг. Оно породило и продолжает порождать переосмысление фундаментальных понятий о неприкосновенности частной жизни и о балансе между безопасностью и свободой в демократическом обществе.

«Вопрос в том, – рассуждает Рональд Ривест, профессор информатики Массачусетского технологического института и один из ведущих американских специалистов по криптографии, – смогут ли люди общаться, не находясь при этом под наблюдением правительства, даже если таковое наблюдение полностью одобрено судебным решением».[1] В атмосфере, создавшейся после 11 сентября 2001 года и породившей Патриотический акт, трудно было поверить, что Конгресс ответит на вопрос профессора Ривеста утвердительно. Однако рыночная действительность дала свой ответ.

---

[1] Заявление Рона Ривеста (Ron Rivest) на пресс-форуме, Массачусетский технологический институт 7 апреля 1998 года.

Чтобы удовлетворить нужды электронной коммерции, криптографическое программное обеспечение должно быть широко доступно. Оно должно работать быстро и надежно, обеспечивая устойчивость к взлому. Кроме того, хотя история криптографии насчитывает не менее четырех тысяч лет, ни один из методов шифрования до конца двадцатого века не мог быть использован для ведения электронной коммерции. Однако в 1976 году двое молодых математиков, даже не работающих в разведке, – вот уж где действительно должны развиваться методы шифрования! – опубликовали статью, описывающую кажущуюся абсурдной реальность. Две стороны разрабатывали секретные ключи, позволявшие обмениваться зашифрованными сообщениями – даже если стороны никогда не встречались, а сообщения пересылались по открытым каналам. Разработанный метод *шифрования с открытым ключом* позволил любому мужчине, женщине или ребенку передавать номера кредитных карт интернет-магазину Amazon более безопасно, чем какой-нибудь генерал мог передавать свои приказы, от которых зависело выживание или уничтожение нации, еще 50 лет назад.

История криптографии

Криптография (от греч. «тайнопись») почти ровесница письменности. Существуют шифрованные сообщения в египетских иероглифах, нанесенные за две тысячи лет до нашей эры. *Шифрование* – это метод преобразования сообщения в непонятную форму, так чтобы восстановление исходного сообщения было возможным. Светоний, биограф Юлия Цезаря, описал его метод шифрования писем к оратору Марку Цицерону, с которым Цезарь обсуждал планы на будущее в последние дни Римской республики: «Если нужно было сообщить что-нибудь негласно, он пользовался тайнописью, то есть менял буквы так, чтобы из них не складывалось ни одного слова. Чтобы разобрать и прочитать их, нужно читать всякий раз четвертую букву вместо первой, например D вместо A и т. д.».[1] Другими словами, Цезарь применял побуквенное шифрование:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Чтобы зашифровать сообщение по методу Цезаря, замените каждую букву верхнего ряда соответствующей буквой из нижнего ряда. К примеру, начало «Записок Цезаря» «Gallia est omnis divisa in partes tres» (Галлия по всей своей совокупности разделяется на три части) будет зашифровано следующим образом:

```
Открытый текст:        GALLIA EST OMNIS DIVISA IN PARTES TRES
Зашифрованный текст:   JDOOLD HVW RPQLV GLYLVD LQ SDUWHV WUHV
```

[1] Гай Светоний Транквилл «Жизнь двенадцати цезарей: Божественный Юлий», часть 56, «Наука», 1993.

Оригинальное сообщение называется *открытым текстом*, а кодированное – *зашифрованным текстом* (или *шифртекстом*). Сообщение расшифровывается с помощью обратной подстановки.

Этот метод называется *сдвигом Цезаря*, или *шифром Цезаря*. Запомнить правило применения метода легко: сдвиньте алфавит трижды. Конечно, можно выполнить сдвиг большее или меньшее число раз. Алфавит Цезаря является целой семьей шифров с числом вариаций 25, по одной для каждой из возможностей сдвига латинского алфавита.[1]

Шифр Цезаря довольно прост; противник, знающий, что применен шифр Цезаря, может легко декодировать сообщение, перебрав все варианты сдвига. Но метод Цезаря является представителем целого класса *шифров простой замены*, в которых одна буква сопоставляется другой по общему правилу (так что одна и та же буква всегда «переводится» одинаково).

Шифров замены может быть создано гораздо больше, чем шифров с применением сдвига. К примеру, можно установить такое соответствие букв английского алфавита:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
XAPZRDWIBMQEOFTYCGSHULJVKN
```

так что **A заменяется на X, B – на A, C – на P и т. д. Это простой способ** замены перестановкой символов алфавита. Число возможных перестановок равно

$26 \times 25 \times 24 \times \cdots \times 3 \times 2$,

то есть примерно 4×10^{26} вариантов, что в 10 тысяч раз больше числа звезд в нашей Вселенной. Такое число перестановок перебрать невозможно. Шифр простой замены должен быть очень надежным – так казалось.

Взлом шифров замены

Примерно в 1392 году некий английский автор – раньше считалось, что это великий английский поэт Джеффри Чосер, – составил письменное руководство по работе с астрономическим прибором. Части этого руководства, озаглавленного **«The Equatorie of the Planetis»** (Движение планет)[2], были закодированы с помощью шифра замены (рис. 5.1). Загадка является более простой, чем кажется на первый взгляд, при

---

[1] В римском алфавите не было символов «J», «U» и «W», поэтому Цезарю были доступны лишь 22 сдвига.

[2] Folio 30 verso of Peterhouse MS. 75.I. Обсуждение авторства Чосера см. Дерек Дж. Прайс (Derek J. Price) «The Equatorie of the Planetis» (Движение планет), Cambridge University Press, 1955 и Кари Энн Рэнд Шмидт (Kari Anne Rand Schmidt) «The Authorship of The Equatorie of the Planetis» (Авторство «Движения планет»), Chaucer Studies XIX, D.S. Brewer, 1993.

том что в ней не так уж много текста, с которым можно работать. Известно, что текст написан на средневековом английском; посмотрим, что можно извлечь из этого факта.

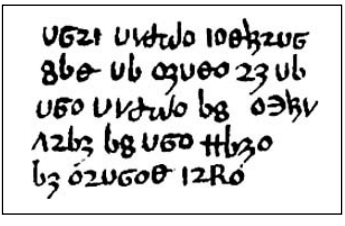


Рис. 5.1. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»*

*Peterson **MS 75.1, том 30v. «The Equatorie of Planetis», манускрипт XIV века,** хранится в Кембриджском университете*

Хотя текст выглядит совершенно бессмысленным, в нем есть несколько ключевых элементов, за которые можно зацепиться. Например, определенные символы встречаются чаще других. В тексте насчитывается 12 символов **0** и 10 символов **U**; никакие другие символы не встречаются так же часто. В обычном тексте на английском языке чаще всего встречаются буквы **E и T, так что можно предположить, что упомянутые** символы соответствуют этим двум буквам. На рис. 5.2 показано, что произойдет, если предположить, что **0**=E и **U**=T. Сочетание **UG0** встречается дважды и представляет трехбуквенное слово T?E. Это может быть **TIE («связь») или TOE («носок обуви»), но слово THE (указательная частица)** кажется более вероятным; следовательно, **G**=H.

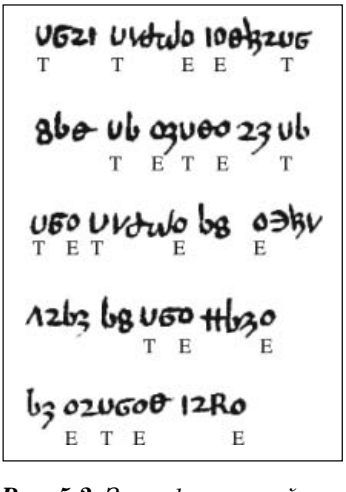


Рис. 5.2. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»**: предполагается, что два наиболее часто встречающихся символа** представляют собой буквы **E и T***

Если это верно, то что это за четырехбуквенное слово в начале текста, начинающееся с TH? Это не THAT (местоимение «тот»), так как оканчивается пока неизвестным символом, и не THEN («тогда»), поскольку третий символ тоже неизвестен. Возможно, здесь зашифровано слово THIS (местоимение «этот»).

И еще есть двухбуквенное слово, начинающееся с T, встречающееся дважды во второй строке. Это должно быть TO (предлог «в» или обозначение неопределенной формы глагола). Результаты частичной расшифровки показаны на рис. 5.3.

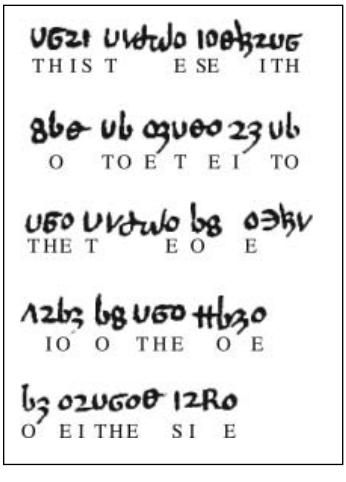


Рис. 5.3. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**»: **расшифрованы другие символы***

Расшифровка пошла на лад. Возможно, последние два слова – это EITHER SIDE, так что оставшиеся символы, зная средневековый английский и общую тематику текста, можно расшифровать без труда. Полностью декодированная фраза выглядит так: «THIS TABLE SERVITH FOR TO ENTRE IN TO THE TABLE OF EQUACION OF THE MONE ON EITHER SIDE» (данные из этой таблицы необходимо ввести в таблицу положений луны с любой стороны) (рис. 5.4).

Данный метод расшифровки называется *статистическим анализом*: если в зашифрованном тексте просто одни буквы заменены другими, то их соответствие можно установить, подсчитав, как часто те или иные буквы встречаются в тексте. Впервые эта идея была высказана арабским философом и математиком Аль-Кинди, жившим в Багдаде в IX веке.

В эпоху Возрождения этот способ расшифровки превратился в разновидность изящного искусства и стал широко применяться в европейских правящих кругах. Известный результат излишнего доверия ненадежным шифрам замены – казнь Марии Стюарт, чья переписка

Рис. 5.4. *Зашифрованный текст из манускрипта «**The Equatorie of Planetis**» расшифрован полностью*

с заговорщиками попала в руки королевы Елизаветы I. Мария Стюарт поплатилась головой за доверие данному способу скрытия тайн; однако шифры замены были популярны вплоть до XIX века, хотя их ненадежность была выявлена еще тысячу лет назад. Сюжеты рассказа Эдгара Аллана По «Золотой жук» (1843) и рассказа Артура Конана Дойля «Пляшущие человечки» (1903) из историй о Шерлоке Холмсе основаны на статистическом декодировании шифров замены.

Секретные ключи и одноразовые шифры

В прикладной криптографии каждый случай взлома кода порождает новый способ защиты от взлома. Убедившись, как просто взломать шифр астрономического манускрипта, мы можем попробовать найти способ сделать шифр более *стойким*, как говорят криптологи. Например, можно заменять одну букву несколькими.

Метод, носящий имя французского дипломата XVI века Блеза де Виженера, использует множество шифров Цезаря. К примеру, можно взять 12 шифров Цезаря и использовать первый шифр для кодирования 1-й, 13-й и 25-й букв открытого текста, второй шифр – для кодирования 2-й, 14-й и 26-й букв и так далее. На рис. 5.5 показан пример шифра Виженера. Открытое сообщение, начинающееся со слова «SECURE...», превратится в «llqgrw...» – как показано на рис. 5.5, S заменяется соответствующим символом из первого ряда, E – из второго и так далее. После достижения нижнего ряда необходимо снова вернуться к первому ряду и повторять процесс замены, пока не будет зашифрован весь открытый текст.

Рис. 5.5. *Шифр Виженера. Ключ к шифру – сочетание «**thomasbbryan**» – находится во второй колонке. Каждый ряд представляет собой шифр Цезаря, в котором величина сдвига определяется соответствующей буквой ключа. (**thomasbbryan – Томас Б. Брайен, адвокат, применивший данный шифр для** переписки со своим клиентом Гордоном МакКеем в 1894 году)*

Архив Гарвардского университета

Чтобы применить шифр с рис. 5.5, не нужно пересылать корреспонденту всю таблицу. Вторая колонка таблицы образует сочетание «thomasbbryan», которое и является ключом. Корреспондентам необходимо только условиться о ключе. Затем на основе ключа создается подстановочная таблица для шифрования и дешифрования сообщений.

Если слово «SECURE» зашифровывается в «llqgrw», то каждая из букв E кодируется разными буквами шифртекста; также буква l шифртекста представляет различные буквы открытого текста – S и E. Таким образом, шифр Виженера делает бесполезной попытку дешифрования с помощью статистического анализа, который в то время был главным инструментом криптоаналитиков. Хотя идея кажется очень простой, открытие Блеза де Виженера явилось прорывом в криптографии, и в течение нескольких сотен лет шифр считался абсолютно стойким (то есть невзламываемым).

Криптологи моделируют операции пересылки зашифрованных данных с помощью шаблонных персонажей: Алиса отправляет сообщение, Боб его получает, а Ева – противник, который может подключиться к каналу связи.

Предположим, Алиса хочет передать Бобу сообщение (рис. 5.6). Здесь подходит метафора «замок–ключ»: Алиса помещает сообщение в ящик и запирает его ключом, который есть только у нее и у Боба (допустим, что замок ящика запирается и отпирается только ключом). Если Ева перехватит ящик по дороге, то не сможет открыть замок без ключа. А Боб, получив ящик, сможет открыть замок своим ключом. До тех

Рис. 5.6. *Стандартный сценарий пересылки зашифрованных данных. Алиса собирается передать сообщение Бобу и зашифровывает текст секретным ключом. Боб дешифрует текст с помощью своей копии ключа. Ева (противник) перехватывает зашифрованное сообщение и пытается восстановить исходный текст*

пор пока форма ключа хранится в тайне, не имеет значения тот факт, что посторонние могут осматривать ящик снаружи или даже узнать принцип конструкции замка. Аналогично, если некий текст закодирован шифром Виженера, восстановить текст, не зная ключ шифра, почти невозможно.

Или, по крайней мере, так считалось. В действительности, шифр Виженера был взломан в середине XIX века английским математиком Чарльзом Бэббиджем, которого ныне считают создателем вычислительных машин. Бэббидж выяснил, что если возможно угадать или как-то вычислить длину ключа и соотнести ее с цикличностью повторения шифра, то проблема взлома сводится к нахождению всего нескольких подстановок. Чтобы вычислить длину ключа, Бэббидж применил статистический анализ. Математик так и не опубликовал свой метод (возможно, под давлением службы разведки).[1] Независимо от Бэббиджа офицер прусской армии Вильям Казиский нашел способ взлома шифра Виженера и опубликовал его в 1863 году. С этого времени использование шифра Виженера перестало быть безопасным.

Надежный способ защиты от взлома шифра Виженера заключается в использовании ключа, длина которого равна числу символов в сообщении; таким образом, шифр не повторяется. Если нам необходимо зашифровать 100 символов, нужно взять 100 шифров Цезаря и расположить их в 100 рядов подобно таблице на рис. 5.5. Каждый ряд будет использован только один раз. Такой метод назван *шифром Вернама*, по имени работавшего после Первой мировой войны изобретателя и сотрудника телеграфной компании AT&T telegraph Гилберта Вернама; также метод широко известен под названием *одноразового шифра*.

[1] О работе Ч. Бэббиджа в этом направлении стало известно только в 1970-х.

Криптография в истории

Криптография (шифрование) и криптоанализ (дешифрование, взлом шифров) были в центре многих поворотных событий человеческой истории. Тесное переплетение дипломатии, войн и технологий шифрования увлекательно описаны в книгах Дэвида Кана (David Kahn) «The Codebreakers» («Взломщики кодов») и Саймона Сингха (Simon Singh) «The Code Book» (Книга шифров).

Термин «одноразовый шифр» происходит от одного из способов реализации его применения. Предположим, что и у Алисы, и у Боба есть по одинаковому блокноту, на каждой странице которого написан уникальный ключ шифра. Алиса зашифровывает сообщение ключом с первой страницы. Боб расшифровывает сообщение тем же ключом. После этого страницы из обоих блокнотов вырываются и уничтожаются. При этом важно заметить, что каждый ключ используется однократно и не создает статистических шаблонов, по которым был взломан шифр Виженера.

Одноразовые шифры применялись во время Второй мировой войны и в период «холодной войны» в форме брошюр, заполненных цифрами (рис. 5.7). В настоящее время власти также используют одноразовые шифры для важных сеансов связи. При этом генерируется множество ключей, передаваемых адресату на компакт-дисках (CD или DVD).

Одноразовый шифр, если им правильно пользоваться, не может быть взломан методами криптоанализа. В шифртексте просто не окажется шаблонов, которыми можно будет воспользоваться. В 1949 году Клод Шеннон открыл важную связь между теорией информации и криптографией.[1] (На самом деле, как раз исследования методов криптографии для военных нужд, которыми занимался Клод Шеннон, и привели к рождению его теории информации и связи.) Ученый математически доказал то, что казалось правильным интуитивно: в теории, одноразовый шифр является абсолютно стойким.

Но, как сказал Йоги Берра[2], «в теории нет разницы между теорией и практикой. На практике такая разница есть». Надежные одноразовые шифры трудно создавать. Если шифр содержит повторы или шаблоны, то, по Шеннону, одноразовый шифр перестает быть стойким. Более важным является то, что пересылка ключа между сторонами без потери или перехвата – трудная задача. Обыкновенно стороны долж-

[1] Клод Шеннон «Теория связи в секретных системах» по изданию: Клод Шеннон «Работы по теории информации и кибернетике», М., ИЛ, 1963.

[2] Йоги Берра (Yogi Berra) – знаменитый американский бейсболист, известный также своими ироническими высказываниями. – *Прим. перев.*

Рис. 5.7. *Немецкий одноразовый шифр, используемый для связи между Берлином и Сайгоном в 1940-е годы. На обложке предупреждение: «Использованные страницы могут содержать шифры сообщений, которые еще не были доставлены. Следует хранить страницы в течение времени, превышающего время доставки сообщений»*

Агентство национальной безопасности США

ны заранее передать ключи и надеяться на их успешную доставку. Длинные ключи труднее передать, чем короткие, так что появляется представляющий серьезную угрозу безопасности соблазн использовать ключи повторно.

КГБ СССР поддался этому искушению, что позволило разведкам Великобритании и США полностью дешифровать свыше трех тысяч дипломатических и агентурных сообщений в период с 1942 по 1946 годы.[1] Проект Агентства национальной безопасности США под названием «VENONA» был рассекречен в 1995 году. Из открытых материалов стало известно, что благодаря работе участников проекта были раскрыты агенты КГБ Клаус Фукс и Ким Филби. Советские сообщения шифровались в два этапа, с применением одноразовых шифров. Это невообразимо затрудняло работу криптоаналитиков, но из-за военных потерь и нехватки ресурсов шифры использовались повторно.

Поскольку практически реализовать абсолютно стойкий шифр трудно, в настоящее время почти все системы шифрования используют относительно короткие ключи. Однако не следует определять надежность только по длине ключа. Сегодня в Интернете можно найти программы, которые взламывают шифр Виженера, и ни один профессиональный шифровальщик не станет его применять. Современные сложные

[1] *www.nsa.gov/publications/publi00039.cfm.*

шифры – отдаленные потомки старых шифров замены. В современных средствах шифрования открытый текст обрабатывается не посимвольно, а блоками. Текст (точнее, битовая последовательность) преобразуется в соответствии с некоторым методом, зависящим от ключа. Сам ключ также является битовой последовательностью, которую Алиса и Боб должны хранить в тайне от Евы. В отличие от шифра Виженера, нет известных (по крайней мере, общественности) методов взлома современных шифров, а наиболее эффективный метод дешифрования сообщения заключается в «лобовой атаке» (brute-force attack) – полном и прямом переборе всех возможных ключей.

Объем вычислений, необходимый для восстановления текста из зашифрованного сообщения путем прямого перебора, экспоненциально возрастает с увеличением длины ключа. Увеличение длины на один бит удваивает объем вычислений на компьютере взломщика, почти не требуя дополнительного времени на шифрование и дешифрование. Именно это делает современные средства шифрования столь полезными: скорость компьютеров может расти – даже экспоненциально, – но объем вычислений для взломщика возрастает так же экспоненциально при использовании ключей все большего размера.

Уроки для эпохи Интернета

Прервем ненадолго повествование, чтобы обсудить некоторые уроки из истории криптографии – принципы, которые были четко формализованы в начале XX века. В конце XX века, когда криптография сильно изменилась благодаря современным компьютерным технологиям и новым алгоритмам шифрования, эти уроки все еще остаются актуальны. А их очень часто прогуливают!

Прорывы случаются, но вести доходят медленно

Марию Стюарт обезглавили, потому что ее переписка с заговорщиками против Елизаветы I была расшифрована при помощи статистического анализа, описанного Аль-Кинди за девять столетий до упомянутых событий. Еще более древние методы оставались в строю до наших дней даже в критических коммуникациях. Светоний описал шифр Цезаря в I веке н. э. Даже два тысячелетия спустя сицилийская мафия использовала эти шифры. Печально известному главарю мафии Бернардо Провенцано удавалось ускользать от итальянской полиции в течение сорока трех лет. Но в 2002 году у одного из соучастников Провенцано нашли несколько *pizzini* – небольших бумажных листков с зашифрованным текстом. Эти листки содержали часть переписки Бернардо с сыном Анжело[1], зашифрованной по методу Цезаря, точно как описано у Светония. Провенцано стал использовать более безопасный шифр,

[1] Росселла Лоренци (Rossella Lorenzi), «Discovery News», 2007 год.

но падение началось. Преступник был обнаружен в жилом доме на ферме и арестован в 2006 году.

Даже ученые не застрахованы от простейших ошибок. Хотя Чарльз Бэббидж и Вильям Казиский взломали шифр Виженера в середине XIX века, научный журнал «Scientific American» полвека спустя описал этот шифр как «невзламываемый» (impossible of translation).[1]

Зашифрованные сообщения обычно кажутся непереводимыми. Небрежный человек, наивный или умудренный опытом, глядя совершенно непонятную смесь букв и цифр, может попасть под ложное впечатление о безопасности. Но криптография – наука, и криптологи знают много способов взломать шифр.

Доверять хорошо, но лучше знать

Нет никаких гарантий того, что даже лучшие современные шифры не могут быть взломаны или уже не являются таковыми. Некоторые шифры имеют под собой серьезную математическую основу, но проверка ее «на прочность» требует серьезного прорыва в математике. Если кто-то и знает, как взломать современные шифры, то этот кто-то наверняка работает в Агентстве национальной безопасности или аналогичном учреждении, а тамошний народ не привык выступать на публике.

В отсутствие строгого доказательства криптостойкости шифра вам остается только полагаться на Главный принцип криптографии: *«Если множество умных людей не смогло решить проблему, значит это неразрешимая (в ближайшее время) проблема».*[2]

Конечно, этот принцип не очень хорош для практики – прорывы в науке по определению не происходят «по заказу» или «в ближайшее время». И когда они случаются, у криптографического сообщества в очередной раз начинают болеть головы. В августе 2004 года на ежегодной конференции по криптографии группа исследователей сообщила о взломе популярного алгоритма MD5, применяемого для компьютерных криптографических операций вроде проверки подписи (message digest), составляющих основу систем безопасности большинства веб-серверов, приложений, требующих ввода пароля, и офисных программных пакетов. Криптологи порекомендовали более безопасный алгоритм SHA-1, но и в нем спустя год обнаружились критические уязвимости.

---

[1] «A new cipher code» (Новый шифр), приложение к «Scientific American», v.58 (27 января 1917 года), с. 61. Из материалов заседаний Клуба инженеров Филадельфии (Библиотека деловой литературы Бейкер, историческое собрание, только по предварительной записи), *www.nku.edu/~christensen/Sciamericansuppl17january1917.pdf.*

[2] Чарли Кауфман, Радиа Перлман, Майк Специнер (Charlie Kaufman, Radia Perlman, Mike Speciner) «Network Security: Private Communication in a Public World» (Сетевая безопасность: частное общение в общественном мире), Prentice-Hall, 1995, с. 40.

Надежный алгоритм шифрования – нечто вроде Святого Грааля компьютерных наук.

Надежный алгоритм шифрования – нечто вроде Святого Грааля компьютерных наук. Каждая обнаруженная уязвимость в принятых шифрах порождает новые идеи по совершенствованию алгоритмов. Мы еще не приблизились к совершенству, но прогресс идет.

Мало иметь надежную систему – нужно ее использовать

Прежде чем выяснять, возможна ли абсолютно безопасная система шифрования, подчеркнем, что даже совершенная математическая модель не обеспечит полную секретность, если ей не следовать.

Блез де Виженер опубликовал свой метод шифрования в 1586 году. Однако военные шифровальщики старались уклониться от применения шифра Виженера, потому что этот метод довольно неудобен в обращении. Шифровальщики пользовались простыми шифрами замены, зная, что они давно взломаны, – надеялись на авось. К началу XVIII века в большинстве европейских стран были организованы так называемые черные кабинеты, через которые проходила вся дипломатическая почта для досмотра и шифрования. Спустя какое-то время дипломаты переключились на шифры Виженера и продолжали шифровать ими документы даже после публикации сведений по технологии взлома.

Сегодня ничего не изменилось. Технологическое решение – неважно, насколько оно хорошо на бумаге, – не будет использоваться, если оно неудобно или дорого. Применение уязвимых систем часто пытаются объяснить попытками избавиться от проблем, связанных с переходом на более безопасные альтернативы.

В 1999 году для защиты домашних и офисных беспроводных соединений был принят стандарт шифрования WEP (Wired Equivalent Privacy). В 2001 году в стандарте WEP были обнаружены серьезные недостатки, позволявшие довольно легко подключаться к беспроводной сети[1], что сразу стало всем известно. Несмотря на это, производители средств беспроводной связи продолжали продавать продукцию, основанную на стандарте WEP, в то время как «знатоки» убеждали покупателей, что «WEP – это лучше, чем ничего». Новый стандарт защищенных беспроводных соединений WPA (Wi-Fi Protected Access) был представлен в 2002 году, но производство новых, сертифицированных для использования со стандартом WPA средств связи началось только в сентябре 2003 года. Хакеры украли более 45 миллионов номеров кредитных карт клиентов сетевого ритейлера TJX, поскольку компания

[1] Никита Борисов, Ян Голдберг, Дэвид Вагнер (Nikita Borisov, Ian Goldberg, and David Wagner) «Intercepting Mobile Communications: The Insecurity of 802.11» (Перехват мобильной связи: уязвимость стандарта 802.11), материалы Седьмой ежегодной международной конференции по мобильным вычислениям и сетям, 16–21 июля 2001 года.

использовала уязвимый стандарт WEP вплоть до 2005 года. Стоимость пренебрежения безопасностью составила сотни миллионов долларов.

Похожим образом дело обстоит со множеством современных устройств типа смарт-карт, основанных на технологии RFID. В январе 2005 года компьютерные исследователи из университета Джона Хопкинса и организации RSA Data Security объявили о взломе автомобильной противоугонной сигнализации, основанной на технологии RFID, и электронной платежной системы, встроенной в миллионы автомобильных RFID-меток. На демонстрации была проведена закупка бензина на станции Exxon/Mobile. Представитель разработчика системы, корпорации Texas Instruments, заметил, что методы исследовательской группы «недоступны большинству исследователей» и заявил: «Не вижу никаких причин изменять наш подход».[1]

Когда шифрование было уделом только военных, начальник, определив факт взлома противником системы безопасности, мог приказать подчиненным использовать новый шифр. Опасность применения слабого шифрования в наши дни основана на трех факторах: высокой скорости распространения новостей об обнаруженных уязвимостях среди экспертов, низкой скорости реакции обывателей и широте распространения криптографического программного обеспечения. Когда университетский исследователь находит в алгоритме небольшую проблему, компьютеры по всему свету становятся уязвимыми, и нет никакого центрального командного пункта, который мог бы издать приказ о всеобщем обновлении программного обеспечения.

Противник знает вашу систему

Последний урок истории криптографии может показаться не столь очевидным. Он состоит в том, что метод шифрования, в особенности разработанный для широкого применения, следует считать более надежным, если он распространен и не был взломан, чем если метод хранится в секрете.

Фламандский лингвист Аугуст Керкхоффс привел этот принцип в своем эссе по военной криптографии в 1883 году.[2] Как он объяснил:

> Система не должна быть секретной и ее попадание в руки противника не должно вызывать беспокойства... Под системой я подразумеваю не

---

[1] «RFID crack raises spector [sic] of weak encryption: Steal a car – and the gas needed to get away» (Взлом RFID вскрывает спектр слабых шифрованных защит: кража автомобиля и топлива, чтобы уехать), *Computerworld* от 17 марта 2005 года, *www.computerworld.com/mobiletopics/mobile/technology/story/0,10801,100459,00.html*.

[2] Аугуст Керкхоффс (Auguste Kerckhoffs) «La cryptographie militaire» (Военная криптография), *Journal des sciences militaires*, т. IX, с. 5–38, январь 1883, с. 161–191, февраль 1883, *www.petitcolas.net/fabien/kerckhoffs/crypto_militaire_1.pdf*.

> ключ, но материальную часть системы: таблицы, словари или необходимые механизмы. Не следует волноваться попусту или подозревать в неблагонадежности работников или подчиненных, зная, что если система, требующая секретности, окажется в руках множества людей, то ее надежность не будет зависеть от степени причастности каждого из них.

Другими словами, если метод шифрования широко распространен, то нереально ожидать, что он надолго останется в секрете. Метод должен разрабатываться так, чтобы оставаться безопасным, даже если все его составляющие (кроме одной – ключа) станут известны.

Клод Шеннон повторил принцип Керкхоффса в своей статье по теории связи в секретных системах: «Предположим, что *противнику известна используемая система*». Клод Шеннон писал:

> Наше ограничение обычно в криптологических исследованиях. Оно является пессимистичным, но безопасно и в конечном счете реалистично, так как можно ожидать, что противник рано или поздно раскроет любую секретную систему.[1]

В современной практике безопасности Интернета принципом Керкхоффса часто пренебрегают. Новые компании нередко делают громкие заявления о создании совершенно нового закрытого метода шифрования, объясняя свой отказ выставить метод на суд общественности необходимостью хранения секрета ради безопасности. Криптологи обычно воспринимают такую «секретность на основе туманности» с большой долей скепсиса.

Даже серьезные организации иногда упускают из вида принцип Керкхоффса. Система защиты цифрового медиасодержания CSS (Content Scrambling System), используемая при записи на диски DVD (Digital Versatile Disc, цифровой многоцелевой диск), была разработана консорциумом киностудий и производителей электроники в 1996 году. Система CSS шифрует содержимое диска, чтобы ограничить неправомерное копирование. Метод шифрования хранился в секрете, чтобы предотвратить производство нелицензионных DVD-проигрывателей.[2] Алгоритм работы системы CSS, который никогда серьезно не исследовался профессиональными криптологами, оказался слабым и был взломан спустя три года после анонсирования. В настоящее время в Интернете можно без труда найти как программы для обхода защиты

---

[1] Статья «Теория связи в секретных системах» из сборника К. Шеннона «Работы по теории информатики и кибернетике». М., ИЛ, 1963.

[2] Джеффри А. Блум, Ингемар Дж. Кокс, Тон Калкер, Жан-Поль М. Ж. Линнарц, Мэтью Л. Миллер, С. Брендан Тро (Jeffrey A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul M.G. Linnartz, Matthew L. Miller, and C. Brendan Traw) «Copy Protection for DVD Video» (Защита от копирования DVD-видео), материалы IEEE, том 87, № 7, июль 1999 года, с. 1267–1276.

CSS, так и множество фильмов с дисков DVD со снятой защитой (более детально защита от копирования обсуждается в главе 6).

Принцип Керкхоффса закрепился в форме стандартов шифрования. Стандарт DES (Data Encryption Standard) был принят в качестве национального стандарта США в 1970-х и широко применялся в коммерческих и финансовых сферах. Стандарт успешно выдержал все попытки взлома, хотя закон Мура сделал процесс перебора всех ключей DES в настоящее время практически осуществимым. Новый стандарт шифрования AES (Advanced Encryption Standard) был принят в 2002 году после тщательной и открытой для общественности проверки.[1] Стандарты DES и AES широко используются и определенно обеспечивают достаточный уровень безопасности. Их алгоритмы шифрования были проверены как профессионалами, так и любителями, и не было замечено никаких серьезных уязвимостей.

Эти уроки так же актуальны сегодня, как и всегда. Но в наше время произошли фундаментальные изменения в криптографии. В конце XX века криптографические методы перестали быть исключительно государственными секретами, став потребительским товаром.

Открытие, навсегда изменившее криптологию

В течение четырех тысяч лет криптография была нацелена на то, чтобы Ева не могла прочитать *перехваченные* сообщения Алисы Бобу. Усилия по шифрованию оказывались тщетными, если ключ попадал в руки противника. Хранение ключа в тайне было делом чрезвычайно важным и довольно рискованным.

Если Алиса и Боб совместно выработали ключ при личной встрече, то как мог Боб сохранить ключ в тайне во время опасного путешествия? Безопасность ключа всегда была исключительно важным приоритетом военной и дипломатической службы. Пилотам и солдатам при угрозе гибели или плена предписывалось в первую очередь уничтожить блокнот с ключом. Раскрытие ключа могло стоить жизни тысячам людей. Безопасность ключа была всем.

Если Алиса и Боб никогда не встречались, то как они могли выработать общий ключ, *не имея* безопасных средств его передачи? Это было фундаментальным ограничением: безопасная связь была практически осуществима только для сторон, которые могли заранее встретиться или использовать общий безопасный метод обмена ключами (например, такой, как диппочта).

Если бы Интернет остановился на этом ограничении, то электронная коммерция никогда бы не получила такого распространения, как сей-

[1] Федеральное издание стандартов № 197, Advanced Encryption Standard, *csrc.nist.gov/publications/fips/fips197/fips-197.pdf*.

час. Пакеты битов, пересылаемые в вычислительных сетях, совершенно не защищены от перехвата.

Но в 1970-х ситуация изменилась. Уитфилд Диффи, 32-летний либеральный математик-теоретик, увлекся криптологией еще будучи студентом Массачусетского технологического института. 31-летний Мартин Хеллман был целеустремленным аспирантом Высшей научной школы Бронкса и профессором в Стэнфорде. Уитфилд Диффи путешествовал по стране в поисках единомышленников по математическим основам криптологии. Найти таких людей было нелегко, поскольку большинство серьезных криптологических исследований велось за закрытыми дверями Агентства национальной безопасности. Ральф Меркль, 24-летний аспирант в области информатики, разрабатывал новый подход к безопасности связи. Сделав одно из важнейших открытий в истории криптографии, Диффи и Хеллман нашли способ практической реализации идей Меркля, представив результат в статье «New Directions in Cryptography» («Новые направления в криптографии»).[1] Описание статьи гласило:

> Способ выработки сторонами секретного ключа, известного только им, путем обмена несекретными сообщениями.

Другими словами, пока Алиса и Боб могут связаться друг с другом, они могут выработать секретный ключ. Не имеет значения, может ли Ева или кто другой прослушивать канал связи. Алиса и Боб используют секретные ключи для шифрования, а Ева не может извлечь из перехваченной информации ничего, что помогло бы установить ключ. При этом Алисе и Бобу совершенно не обязательно встречаться или о чем-то уславливаться заранее.

Важность этого открытия невозможно переоценить. Секретная связь была монополией правительств со времени изобретения письменности – правительство, заинтересованное в сохранении своих секретов, всегда забирает лучших шифровальщиков. Есть и еще одна причина правительственной монополии: только у него достаточно средств, чтобы обеспечить выработку, защиту и передачу ключей. Если бы обычные люди заполучили средства выработки секретных ключей, кто угодно мог бы использовать шифрование. Нужно только знать, как создать ключи; для передачи и защиты ключей не нужны ни дипкурьеры, ни армии.

Диффи, Хеллман и Меркль назвали свое открытие «шифрованием с открытым ключом». Хотя вначале оно не было оценено по достоинству, открытие сделало возможной электронную коммерцию. Представьте себя на месте Алисы, а магазин Amazon – на месте Боба. Как вы могли бы встретиться, чтобы выработать общий ключ? И *есть ли вообще* физическое расположение у магазина Amazon? Если Алиса отправляет

[1] Уитфилд Диффи и Мартин Хеллман (Whitfield Diffie and Martin Hellman) «New directions in cryptography» (Новые направления в криптографии), *IEEE Transactions on Information Theory*, ноябрь 1976.

свой номер кредитной карты по защищенному соединению, шифрование выполняется на логическом узле, точнее, на двух узлах Интернета. Методы Диффи, Хеллмана и Меркля и сопутствующие технологии обеспечили возможность безопасных интернет-транзакций. Покупая товар в интернет-магазине, вы, возможно, сами того не зная, занимаетесь шифрованием. В ролях Алисы и Боба выступают ваш компьютер и сервер магазина.

В 1997 году стало известно, что аналогичные технологии шифрования с открытым ключом были разработаны за два года до открытия Диффи и Хеллмана сотрудниками британского Главного управления правительственной связи (Government Communication Headquarters, GCHQ) Джеймсом Эллисом, Клиффордом Коксом и Малькольмом Уильямсоном.[1]

Кажется совершенно невероятным, что стороны могут выработать секретный ключ посредством открытого канала связи. Могли ли Диффи, Хеллман и Меркль преуспеть в том, что научное сообщество пыталось создать, но потерпело неудачу? А вот и нет, никто и не пытался создать ничего подобного, поскольку казалось очевидным, что Алиса и Боб должны были каким-то тайным образом обменяться ключами.

Даже великий Клод Шеннон упустил из виду это решение. В своей статье, объединившей и поставившей на строго научную основу все известные криптографические методы, Шеннон не предполагал альтернативных возможностей безопасной коммуникации: «Ключ передается некоторым способом на приемный конец, причем предполагается, что его нельзя перехватить».

Стороны могут выработать секретный ключ, даже если все их сообщения перехватываются.

Это не обязательно. Стороны могут выработать секретный ключ, даже если все их сообщения перехватываются.

Базовая схема передачи Алисой ключа Бобу остается такой, как показано на рис. 5.6. Алиса отправляет Бобу зашифрованное сообщение. Боб дешифрует текст с помощью секретного ключа. Шпионка Ева *перехватывает* зашифрованное сообщение и пытается восстановить исходный текст.

Преимуществом подобной системы шифрования является *невозможность* для Евы восстановить текст иначе, чем прямым перебором всех возможных ключей. Здесь на помощь Алисе и Бобу приходит эффект экспоненциального роста. Предположим, к примеру, что стороны ис-

[1] Джеймс Эллис (James Ellis) «The History of Non-secret Encryption» (История несекретного шифрования), *www.cesg.gov.uk/site/publications/media/ellis.pdf*.

пользуют в качестве ключа набор из 10 десятичных цифр. Если компьютеры Евы обладают достаточным быстродействием для перебора всех возможных ключей, стороны могут начать использовать ключ из 20 цифр. В таком случае время, требуемое для перебора, возрастает в 10^{10} раз. Если компьютеры Евы могут перебрать ключи первого типа за 1 секунду, то для перебора ключей второго типа теми же средствами потребуется более 300 лет!

Перебор всех возможных значений всегда остается *единственным средством* нахождения ключа для Евы. Но если Алиса закодирует сообщение шифром замены или шифром Виженера, то шифртекст будет содержать статистические закономерности, которые существенно облегчат задачу Евы. Способ защиты состоит в том, чтобы обеспечить полное отсутствие статистических закономерностей в шифртексте.

Протокол соглашения о ключе

Решающее значение имеет концепция *односторонних вычислений* (*односторонней функции*) – вычислений, обладающих двумя важными свойствами: а) прямое вычисление выполняется быстро; б) обратное вычисление выполняется медленно (если вообще выполняется). Более точно, односторонняя функция принимает в качестве аргументов числа x и y и вычисляет третье число, которое обозначим $x \times y$. Если третье число известно, то даже при знании значения x очень трудно найти значение y. Единственный способ найти значение y – метод проб и ошибок. С увеличением количества разрядов числа y время перебора возможных значений возрастает экспоненциально, становясь практически бесконечным для чисел из нескольких сотен разрядов. Еще одно важное свойство односторонней функции Диффи-Хеллмана: результат выражения $(x \times y) \times z$ равен результату выражения $(x \times z) \times y$.

Протокол соглашения о ключе начинается с публичного объявления о способе вычисления $x * y$ и величине некоторого большого числа g[1]. Вся эта информация общедоступна. Зная ее, стороны могут создать защищенный канал связи по следующим шагам.

1. Каждая сторона выбирает случайное число. Обозначим число Алисы буквой a, число Боба – b. Это будут *закрытые ключи* сторон, известные только им.
2. Алиса вычисляет $g \times a$, а Боб – $g \times b$ (это не требует значительных вычислений). Результаты вычислений называются *открытыми ключами* (обозначим их A и B).
3. Алиса отправляет Бобу число A, Боб отправляет Алисе число B. Не имеет значения, сможет ли Ева получить копии открытых ключей.

[1] Частная односторонняя функция Диффи–Хеллмана – это остаток от деления xy на p, где p – стандартное фиксированное число.

4. После получения открытого ключа B Алиса вычисляет значение $B \times a$; аналогично, Боб вычисляет значение $A \times b$.

Хотя стороны выполняют вычисления с разными величинами, но получают одинаковые результаты. Боб вычисляет значение $A \times b$, то есть, $(g \times a) \times b$ (см. шаг 2). Алиса вычисляет $B \times a$, то есть, $(g \times b) \times a$. В соответствии с третьим свойством односторонней функции, $(g \times a) \times b = (g \times b) \times a$.

Уверены ли мы, что шифр с открытым ключом нельзя взломать?

Несмотря на объединенные усилия лучших математиков и программистов, направленные на достижение абсолютной надежности шифрования, никто еще не доказал математически, что шифр с открытым ключом нельзя взломать. Доверие шифрам покоится на главном принципе «этого еще никто не сделал». Если кто и знает метод быстрого дешифрования, то это, возможно, Агентство национальной безопасности, которое проводит свои исследования в режиме строгой секретности. Если Агентство и знает, то молчит. Возможно, некий изобретатель-одиночка нашел способ взлома, но предпочел славе деньги и тихо наживается, дешифруя финансовые транзакции. А мы остаемся в уверенности, что никто не может и не сможет взломать шифр с открытым ключом.

Это общее число (обозначим его K) является ключом, который стороны используют для обмена зашифрованными сообщениями на основе выбранной функции.

Здесь есть критическая точка. Предположим, что Ева прослушивает канал связи. Что может извлечь Ева из полученных данных? У нее есть A и B, она знает значение g из спецификации стандарта. Ева знает все алгоритмы и протоколы; наконец, она тоже читала статью Диффи и Хеллмана. Но, чтобы вычислить ключ K, Ева должна знать один из секретных ключей – a или b. Но только Алиса знает значение ключа a, и только Боб знает значение ключа b. При использовании чисел из нескольких сотен разрядов невозможно вычислить a или b, зная g, A и B, без перебора практически бесконечного количества возможных вариантов значений.

Выполнять генерацию ключей стороны могут на персональных компьютерах или с помощью специальной аппаратуры. Но даже самые мощные компьютеры не обладают достаточным быстродействием, чтобы третья сторона могла взломать шифр известными методами.

Эта невообразимая разница между прямыми и обратными вычислениями и составляет сущность открытия Диффи, Хеллмана и Меркля. Криптологи смогли найти способ создания общих секретных ключей без необходимости использования безопасных каналов связи.

Открытые ключи для закрытых сообщений

Допустим, Алиса хочет, чтобы кто-то мог отправлять ей зашифрованные сообщения, которые сможет расшифровать только Алиса. Это можно реализовать с помощью небольших изменений в протоколе соглашения о ключе. Вычисления остаются теми же, но происходят в несколько ином порядке.

Алиса формирует закрытый ключ a и вычисляет открытый ключ A. Алиса делает ключ A общедоступным.

Если Боб (или кто-то другой) собирается отправить Алисе шифрованное сообщение, он получает копию ключа A и вычисляет свои ключи b и B. Затем Боб использует ключ A для стандартной операции вычисления ключа $K = A \times b$. Боб шифрует свое сообщение ключом K и отправляет Алисе шифртекст и свой открытый ключ B. Так как ключ K используется только один раз, этот метод можно назвать одноразовым шифром.

Когда Алиса получает шифртекст Боба, она вычисляет (используя свой закрытый ключ a) значение ключа $K = B \times a$, а затем с его помощью дешифрует сообщение. Ева же не может дешифровать сообщение, так как не знает значений ни одного из закрытых ключей.

С помощью технологии шифрования с открытым ключом кто угодно может отправить кому угодно зашифрованное сообщение, используя небезопасные общедоступные средства связи.

Описанный способ может показаться всего лишь вариантом обмена ключами, но этот способ открывает принципиально новое понимание безопасности коммуникации. С помощью технологии шифрования с открытым ключом *кто угодно* может отправить *кому угодно* зашифрованное сообщение, используя небезопасные общедоступные средства связи. Необходимо лишь договориться об использовании метода Диффи-Хеллмана-Меркля и осознать, что все попытки третьей стороны декодировать шифртекст останутся бесплодными.

Цифровые подписи

В дополнение к безопасности коммуникаций применение технологии шифрования с открытым ключом позволяет предотвращать подлоги и подмены участников электронных транзакций.

Предположим, что Алиса собирается сделать публичное заявление. Как люди могут удостовериться, что заявление действительно исходит

от Алисы? Не подлог ли это? Алисе необходимо обеспечить средство, которое позволило бы легко установить, что текст заявления действительно принадлежит ей. Это средство называется *цифровой подписью*.

Вернемся к классическому сценарию: Алиса отправляет сообщение Бобу, а Ева пытается препятствовать пересылке сообщения. В данном случае нас не интересует обеспечение секретности содержимого – только факт установления подлинной личности отправителя. Другими словами, сообщение, например публичное заявление, может и не быть зашифровано. Но Боб должен быть уверен, что подпись на сообщении действительно принадлежит Алисе, а само сообщение никем не искажено.

Протокол передачи подписанного сообщения использует открытый и закрытый ключи, но не так, как при шифровании. Протокол требует выполнения двух вычислений: в первом Алиса обрабатывает сообщение для формирования подписи, во втором Боб проверяет подлинность подписи. Алиса использует само сообщение и свой закрытый ключ, чтобы создать цифровую подпись. После этого любой желающий может получить копию открытого ключа Алисы, чтобы проверить ее авторство. Таким образом, создать подпись может только владелец закрытого ключа, а проверить ее – кто угодно. Этот сценарий обратен предыдущему, в котором любой может отправить создателю открытого ключа шифрованное сообщение, но после зашифровки только владелец закрытого ключа может сообщение декодировать и прочитать.

Модель цифровой подписи требует легкости вычислений как для формирования подписи, так и для ее верификации с помощью открытого ключа и, напротив, формирование ложной подписи без закрытого ключа должно быть практически неосуществимо. Кроме того, подпись опирается на текст сообщения в той же степени, как и на закрытый ключ, – следовательно, протокол передачи подписанного сообщения гарантирует одновременно и *целостность* оригинального текста, и *подлинность автора* (Алисы).

В реальных системах (к примеру, используемых для подписи незашифрованных сообщений электронной почты) Алиса не обрабатывает все сообщение. Вместо этого для увеличения скорости вычислений, Алиса обрабатывает свертку сообщения, называемую *дайджестом*. Дайджест намного короче сообщения, поэтому подпись для дайджеста вычисляется значительно быстрее. Способ вычисления дайджеста является общеизвестным. Получив подписанное сообщение, Боб самостоятельно вычисляет дайджест и сверяет его с результатом дешифрования подписи Алисы при помощи ее открытого ключа.

Процесс формирования цифровой подписи создает нечто вроде отпечатка пальца – нечто небольшое, но уникальным образом идентифицирующее оригинал. Процесс сжатия оригинала несет в себе некоторый риск. Если Ева сможет создать отличное от оригинала сообщение с тем же дайджестом, то сможет прикрепить к своему сообщению подпись

Алисы. Боб не сможет распознать подделку, так как при проверке подписи сделает вывод об авторстве Алисы. Источник риска – небезопасность ранее упоминавшегося в этой главе алгоритма MD5; криптологическое сообщество рекомендует избегать применения дайджестов.

Стандарт шифрования RSA

Диффи и Хеллман анонсировали свою концепцию цифровой подписи в 1976 году. Авторы предложили лишь общий подход без создания конкретной реализации. Задача создания алгоритма формирования цифровой подписи стала достойным вызовом ученым и программистам.

Вызов был принят в 1977 году сотрудниками лаборатории информатики Массачусетского технологического института Роном Ривестом, Ади Шамиром и Леном Адлеманом. Разработанный ими алгоритм RSA (названный по фамилиям разработчиков – Rivest-Shamir-Adleman) позволял как формировать цифровую подпись, так и шифровать. При работе с RSA пользователь генерирует пару ключей: открытый и закрытый. Снова обозначим их A и a соответственно. Открытый и закрытый ключи взаимно дополняют друг друга: если преобразовать открытый текст ключом a, то обработка шифртекста ключом A восстановит оригинал сообщения; и наоборот.

Вот как используются на практике ключи RSA. Пользователи публикуют открытые ключи, а закрытые ключи хранят в тайне. Если Боб хочет отправить Алисе сообщение, то он выбирает стандартный алгоритм, например DES, и формирует ключ K. Затем Боб преобразует K, используя открытый ключ Алисы A. Алиса использует закрытый ключ a, чтобы восстановить K. Как во всех методах шифрования с открытым ключом, только Алиса владеет закрытым ключом и может прочитать сообщение Боба.

Чтобы сформировать цифровую подпись, Алиса преобразует сообщение с помощью закрытого ключа a и использует результат преобразования как подпись, дополняющую сообщение. Адресат может проверить подлинность подписи с помощью открытого ключа A. Так как только Алиса владеет закрытым ключом, то только она могла создать последовательность, которая при обработке ключом A воспроизведет оригинальное сообщение.

Кажется практически неосуществимым вычислить в стандарте RSA закрытый ключ, соответствующий конкретному открытому ключу. Это похоже на алгоритм Диффи-Хеллмана-Меркля, хотя используется другая односторонняя функция. Шифр RSA является стойким, если разложение на множители числа из n разрядов занимает намного больше времени, чем перемножение двух чисел с количеством

Открытие, облегчающее задачу быстрой факторизации, сделало бы слабым шифр RSA – и бесполезными многие текущие стандарты безопасности в Интернете.

разрядов $n/2$. Зависимость стандарта **RSA от трудности факторизации** (операции разложения на множители) породила безмерный интерес к нахождению быстрых способов перемножения чисел. Вплоть до 1970-х это была всего лишь математическая головоломка, представляющая теоретический интерес. Насколько известно, перемножение чисел отнимает время, сравнимое с *количеством разрядов*, а факторизация – сравнимое со *значением* числа.[1] Открытие, облегчающее задачу быстрой факторизации, сделало бы слабым шифр **RSA – и бесполезными** многие текущие стандарты безопасности в Интернете.

Цифровые сертификаты и центры сертификации

Авторы книги уже описывали проблему, возникающую при использовании шифрования с открытым ключом. Как может Боб быть уверен, что «Алиса», с которой он переписывается, – это действительно Алиса? На другом конце канала связи может быть кто угодно. Или после того, как Алиса опубликует свой открытый ключ в общем каталоге, туда наведается Ева и подменит ключ. В результате письма, предназначенные Алисе, сможет прочитать только Ева. Если «Боб» – это вы, а «Алиса» – это мэр, приказывающий начать эвакуацию города, самозванец может выдать себя за мэра и вызвать панику. Если «Боб» – это ваш компьютер, а «Алиса» – это банковский сервер, то злоумышленник может оставить вас без денег!

Здесь могут помочь цифровые подписи. Алиса направляет в проверенный центр сертификации свой открытый ключ и доказательства подлинности ее личности. Центр подписывает ключ Алисы, формируя новый ключ, называемый *сертификатом*. Алиса публикует уже не свой открытый ключ, а сертификат. Тот, кто хочет переписываться с Алисой, первоначально проверяет подпись центра сертификации, чтобы удостовериться в подлинности открытого ключа.[2]

Проверка сертификата выполняется путем проверки подлинности подписи центра сертификации. Можно ли верить результату проверки? Не подделан ли сертификат Евой? Как правило, подпись центра сертификации, в свою очередь, подписана центром более высокого уровня и так далее, с цепочкой подписей вплоть до центра, чья подпись может считаться абсолютно надежной. Таким образом, открытый ключ (теперь уже – сертификат) Алисы защищен от подделки не одной подписью, а целой цепочкой подписей, каждая из которых подтверждает предыдущую.

---

[1] Точнее, время умножения n-разрядных чисел растет линейно, в то время как длительность наиболее быстрых известных алгоритмов разложения на множители растет пропорционально кубическому корню из n.

[2] Эта идея и термин «сертификат» были предложены Лореном Конфельдером в его дипломных тезисах на степень бакалавра в Массачусетском технологическом институте (Loren M. Kohnfelder «Towards a Practical Public-key Cryptosystem», MIT S.B. Thesis, май 1978 года, не опубликовано).

Коммерческие сертификаты

Наиболее влиятельный сегодня коммерческий центр сертификации VeriSign выдает сертификаты трех классов. Сертификат первого класса (Class 1) удостоверяет, что владелец сертификата соответствует данному адресу электронной почты и не содержит никаких подтверждений относительно личности владельца. Сертификат второго класса (Class 2) обеспечивает умеренный уровень подтверждения личности владельца. Организации, выдающие такие сертификаты, требуют представления информации, удостоверяющей личность, вроде справки с работы или кредитной истории. Сертификат третьего класса (Class 3) требует личной явки или предоставления документов, подтверждающих личность.

Организации, выдающие цифровые сертификаты, называются *центрами сертификации* (certification authorities, CA). Центры сертификации могут быть настроены на ограниченное использование (например, корпорация может организовать свой собственный центр для внутренней сети). Также есть компании, получающие прибыль от продажи сертификатов. Ваше доверие цифровому сертификату должно складываться из двух статей: во-первых, из вашего доверия конкретному сертификату, во-вторых, из вашего доверия политике выдачи сертификатов конкретным центром.

Шифрование для всех

В обычной жизни редко кто осознает, что выполняет вычисления значений односторонней функции во время просмотра веб-страниц. Но это именно то, что происходит, когда вы покупаете книгу в магазине Amazon, проверяете баланс кредитной карты или оплачиваете покупку электронными деньгами PayPal. Признаком защищенного соединения является адрес URL веб-сайта, начинающийся с префикса протокола «https» вместо обычного «http» (буква «s» означает secure – безопасный). Без ведома пользователя его компьютер и компьютер банка или интернет-магазина устанавливают зашифрованное соединение. Сайт магазина доказывает свою подлинность путем предоставления сертификата от центра, которому компьютер пользователя настроен доверять. Для каждой новой транзакции генерируются новые ключи; это не требует больших затрат. Повсюду в Интернете передаются секретные сообщения. Теперь все мы – шифровальщики.

Теперь все мы – шифровальщики.

В начале своего существования шифрование с открытым ключом считалось чем-то вроде математической шутки.[1] Лен Адлеман (один из изобретателей стандарта RSA) считал статью об алгоритме RSA «наименее интересной публикацией, к которой я приложил руку». Даже Агентство национальной безопасности, по крайней мере в 1977 году, не приветствовало широкое внедрение шифрования с открытым ключом. Агентство просто не могло радоваться тому, что революция персональных компьютеров сделает возможным для простых людей обмен зашифрованными сообщениями, которые не смогут прочитать даже спецслужбы.[2]

Но с развитием технологий в 1980-х развивался и Интернет, и потенциальные возможности общедоступного шифрования стали очевидны. Спецслужбы все больше беспокоились, а законодатели пугали правительство заявлениями о том, что средства шифрования сделают невозможным применение одного из самых мощных средств власть имущих – прослушивание каналов связи. Выгоду использования секретных коммуникаций ощутили представители бизнеса, в особенности электронной коммерции. На рубеже 1980–1990-х столы администраций президентов Буша и Клинтона были буквально завалены предложениями по контролю применения средств шифрования.

В 1994 году администрация президента Клинтона обнародовала план «Стандарта доверенного шифрования» (Escrowed Encryption Standard, EES), который требовалось использовать в телефонных аппаратах, обеспечивающих зашифрованную связь. Стандарт под названием «Clipper» был реализован Агентством национальной безопасности в виде шифрующей микросхемы, содержащей *«черный ход»* – дополнительный ключ, хранимый в правительственном учреждении и позволявший спецслужбам дешифровать телефонные переговоры. В соответствии с планом правительство закупало для секретной связи только телефоны на основе микросхемы «Clipper». Представители промышленности отнеслись к плану прохладно (рис. 5.8), и инициатива была свернута. Однако в последующих модификациях плана начиная с 1995 года правительство продолжало пытаться убедить производителей создавать средства связи с подобным «черным ходом» в конструкции. В качестве кнута и пряника применялось экспортное законодательство. В соответствии с ним криптографические средства не могли быть экспортированы без лицензии, а игнорирование запрета влекло за собой строгие уголовные меры. Предложение правительства разрешало экспорт только тех средств шифрования, которые содержали «черный ход».

---

[1] *www.channel4.com/science/microsites/S/secrecy/page5b.html*

[2] Беседа Бобби Рэя Инмана и Хэла Абельсона, февраль 1995 года. Вскоре после появления стандарта RSA Агентство национальной безопасности попросило институт не публиковать документацию, но институт отказался, сославшись на научную открытость.

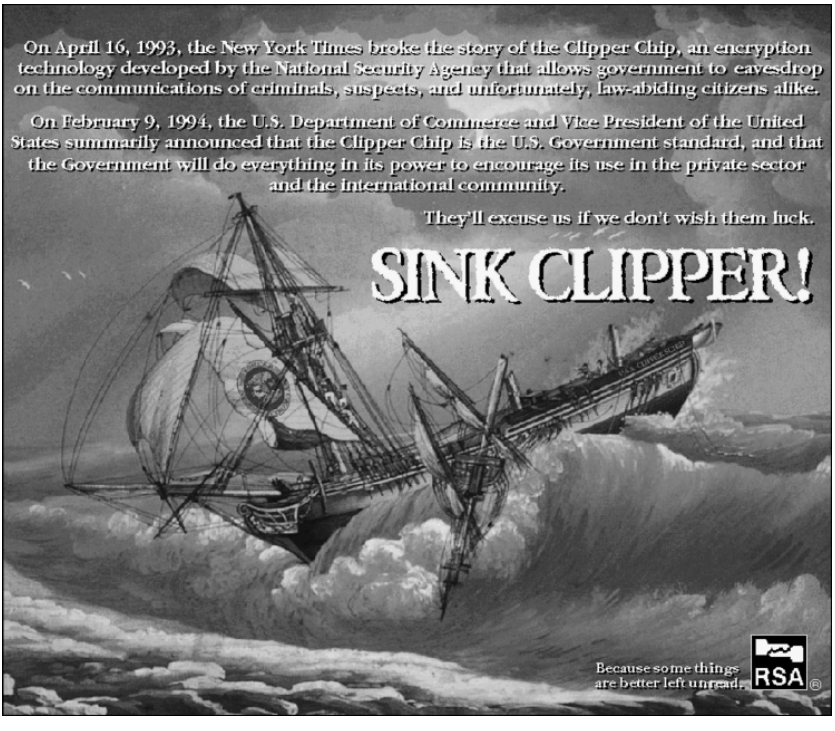


Рис. 5.8. *Артефакт времен «криптографических войн», результат яростной реакции производителей высокотехнологичной продукции на план «Clipper Chip» администрации президента Клинтона*

Повторно публикуется с разрешения правообладателя

Последовавшие за этим дебаты, часто весьма жаркие, вошли в историю под названием «криптографических войн». Напряжение стало спадать лишь в конце 1990-х. Законодатели и службы национальной безопасности высказывались за контроль над средствами шифрования. Их оппоненты – производители высокотехнологичных продуктов и борцы за гражданские права – были против правительственного контроля и расширения возможностей прослушивания. Больше всего представители власти не хотели соглашаться с тем, что важная военная технология может превратиться в рядовой инструмент обывателей.

В начале главы авторы упоминали о Филе Циммерманне, и теперь центром внимания становится его работа. В 1970-е Циммерманн был неплохим программистом и борцом за гражданские права. Шифрованием он интересовался с юности. Статью об алгоритме RSA из журнала *Scientific American* Циммерманн прочитал в 1977 году. В это время у него не было доступа к компьютерам, которые могли бы выполнять требуемые алгоритмом вычисления над многоразрядными целыми

числами. Но вычислительная мощь компьютеров росла, и в 1980-х стало возможным реализовать алгоритм RSA на персональном компьютере. Циммерманн начал разрабатывать гражданские программы для шифрования, чтобы противостоять угрозе расширения возможностей спецслужб по прослушиванию. Из более позднего выступления Циммерманна перед Конгрессом:

> Но такой уровень роста электронного цифрового общения чреват разрушением нашей конфиденциальности. В прошлом, если правительство хотело нарушить право обычных граждан на неприкосновенность частной жизни, оно должно было потратить деньги и усилия на то, чтобы перехватить, открыть над паром и прочитать бумажную почту. Или ему приходилось подслушивать и транскрибировать телефонные разговоры, до тех пор пока не изобрели технологию автоматического распознавания голоса. Этот способ аналогичен ужению рыбы – на один крючок можно поймать только одну рыбу. К счастью для свободы и демократии, такой сложный способ слежения на практике не подходит для широкого использования. Сегодня электронная почта постепенно замещает обычную. Она становится правилом, а не исключением, как раньше. В отличие от бумажной почты, электронную почту просто перехватить и отсканировать на интересующую информацию, что делается легко, ежедневно, автоматически и незаметно. Это аналогично ловле рыбы сетью, оруэлловскому количественному и качественному отбору, подрывающему здоровье демократии.[1]

Ответом на действия правительства стало шифрование. Как только спецслужбы получили неограниченные возможности по прослушиванию электронных каналов связи, гражданам повсеместно потребовалась простая в использовании, недорогая криптостойкая технология, позволяющая общаться так, чтобы прослушивание стало бесполезным.

Перед Циммерманном возникли препятствия, непреодолимые для менее рьяного борца за права. Стандарт RSA был запатентован и лицензирован только для компании RSA Data Security, производившей коммерческие программные продукты для крупного бизнеса. Компания не желала идти навстречу Циммерманну и предоставить ему лицензию на запланированную разработку свободно распространяемых программ.

А еще была правительственная политика, против которой, собственно, и выступал Фил Циммерманн. 24 января 1991 года сенатор Джозеф Байден, соавтор антитеррористического сенатского билля № 266, внес в билль некоторые дополнения:

> Общее мнение собрания Конгресса состоит в том, чтобы поставщики услуг электронной связи и производители коммуникационного оборудования обеспечили меры, согласно которым уполномоченным представителям правительства будут предоставлены распечатки голосовой, передающей данные и иных услуг связи при получении соответствующего официального запроса.

---

[1] *http://www.philzimmermann.com/RU/testimony/index.html*

Правительственный контроль шифрования в мире

В разных странах одни и те же алгоритмы шифрования по-разному применяются для коммерческих, военных и политических целей. Например, китайское правительство строго ограничивает продажу средств шифрования: только для «обеспечения безопасности информации, защиты законных интересов граждан и организаций и гарантии безопасности и интересов нации».[1] В Великобритании в 2007 году приняли закон, требующий принудительной передачи официальным лицам ключей шифров при расследовании уголовных дел (в том числе, связанных с терроризмом) под угрозой лишения свободы сроком до пяти лет.[2]

Эти дополнения вызвали волну протестов со стороны борцов за гражданские права и, казалось, нанесли решающий удар по свободе связи, но Циммерманн решил взяться за дело сам.

В июне 1991 года Циммерманн закончил работу над полнофункциональной версией своей программы, получившей название Pretty Good Privacy (Лучшая приватность) по названию выдуманного спонсора Ralph's Pretty Good Groceries (лучшие бакалейные товары Ральфа) с радиошоу Prairie Home Companion. Программа PGP таинственным образом появилась на нескольких американских серверах, а в скором времени ее копии распространились повсюду. По словам самого Циммерманна, «эта технология принадлежит всему миру». Джинн выбрался из бутылки, и не так-то легко запереть его обратно.

За этот подвиг свободы Циммерманну пришлось заплатить. Компания RSA Data Security не желала делиться технологией шифрования, да еще со «всем миром». Упустив власть над технологией, руководство компании пришло в ярость. Правительство тоже было не в восторге. Против Циммерманна было возбуждено уголовное дело в связи с нарушением экспортного законодательства, хотя было не совсем ясно, какие именно положения закона нарушены. В конце концов владелец патента – Массачусетский технологический институт – предоставил Циммерманну лицензию на использование патента RSA и право на распространение PGP в США в рамках экспортного законодательства.

К концу десятилетия электронная коммерция взяла свое, и правительство прекратило судебное преследование, так и не вынеся обвинительное заключение. Фил Циммерманн создал компанию по платному распространению PGP (загляните на сайт *www.pgp.com*), в то же время сохранив

[1] Директива № 273 о коммерческих шифрах Государственного совета КНР.

[2] Часть 3 секция 49 Акта о регулировании следственных действий (Regulation of Investigatory Powers Act).

возможность бесплатного скачивания для рядовых граждан. Личный сайт Циммерманна содержит рекомендации от организаций по защите гражданских прав из Восточной Европы и Гватемалы, свидетельствующие об успешном использовании шифрованной связи в противостоянии жестким политическим режимам. Циммерманн победил.

Вроде бы.

Настоящее и будущее шифрования

Сегодня шифруется любая кредитная или банковская интернет-транзакция. Многие озабочены информационной безопасностью, кражами идентификационных данных и деградацией отношения к неприкосновенности частной жизни. Для гражданского применения доступны мощные средства шифрования, такие как PGP, и многие из них бесплатны.

Однако до сих пор не шифруется большая часть сообщений электронной почты. Защитники прав и свобод граждан шифруют свою почту. Люди, которым есть, что скрывать, возможно, тоже. Но большинство не заботится о том, чтобы шифровать свои сообщения. Миллионы граждан пользуются почтовым сервисом Gmail, фактически обменивая свою частную жизнь на услуги надежного и бесплатного почтового ящика. Компьютеры корпорации Google сканируют каждое письмо и предлагают пользователю соответствующую рекламу. Архив почтовых сообщений может быть предоставлен властям по судебному запросу. Почему нас так мало волнует безопасность электронной почты?

Почему нас так мало волнует безопасность электронной почты?

Во-первых, пользователей все еще мало волнует то, насколько легко пакеты байтов электронной почты могут быть перехвачены в пути. Запрос пароля, требуемый почтовым сервером, создает иллюзию безопасности, но никак не обеспечивает защиту от перехвата самих сообщений. И не важно, путешествуют ли сообщения по стекловолокну, меди или радиоволнам. Самая мощная в мире система прослушивания все еще малоизвестна. Это международная система ECHELON, которая автоматически обрабатывает потоки интернет-пакетов, передаваемых с помощью орбитальных спутников связи. Система ECHELON является совместным проектом США и нескольких союзных государств; это продолжение послевоенных систем радиоразведки. Система ECHELON аккумулирует передовые технологии связи.[1] Если текст вашего сообщения содержит слова из базы данных системы ECHELON, вами могут серьезно заинтересоваться.

[1] Патрик Рэдден Киф (Patrick Radden Keefe) «Chatter: Dispatches from the Secret World of Global Eavesdropping» (Болтовня: отправки из секретного мира глобального подслушивания), Random House, 2005.

Шпионаж за гражданами

Исторически сложилось так, что шпионаж за гражданами США требует особых полномочий (поскольку у граждан есть право на неприкосновенность частной жизни), но для шпионажа за иностранными гражданами специального разрешения не требуется. Ряд законов и постановлений, направленных на борьбу с терроризмом[1], позволяет спецслужбами проверять потоки битов, направленных как в страну, так и из страны (и даже звонки в авиакомпанию, если на звонок отвечает оператор из индийского центра). Также из общего ряда правовых табу выпадает «наблюдение за лицом, чье обоснованно предполагаемое местоположение находится за пределами Соединенных Штатов», вне зависимости от гражданства вышеупомянутого лица. Развитие законодательства в данном направлении может стимулировать применение гражданских средств шифрования и даже создать обратный эффект – вызвать криминализацию шифрования каналов связи в США.[2]

Во-вторых, большинству граждан особо нечего скрывать, так что им незачем беспокоиться о перехвате сообщений. Пользователи не принимают в расчет растущие возможности властей по тотальному автоматическому мониторингу, о котором предупреждал Циммерманн.

Наконец, шифрование электронной почты не встроено в инфраструктуру Интернета, как это сделано в отношении передачи веб-страниц. Для шифрования почты нужны нестандартные программы, которых может не оказаться у ваших адресатов. В компаниях руководство может возражать против шифрования почты сотрудников. Руководство беспокоится – и часто не без оснований – о возможности противоправных действий работников. Вряд ли кому-то хочется, чтобы нельзя было гарантировать даже под угрозой правового преследования, что корпоративная почта не попадет в чужие руки.

Технически возможно шифровать не только электронную почту или номера кредитных карт. Мгновенные сообщения и данные телефонии VoIP являются всего лишь пакетами байтов и могут быть зашифрованы, как и любые другие данные. Некоторые программы интернет-телефонии (например, Skype) шифруют голосовые данные, в разработке находятся и другие продукты, в том числе проект самого Циммерманна.

---

[1] Акт о защите Америки 2007 года (Protect America Act), § 1927 Акта о внешней разведке (Foreign Intelligence Surveillance Act).

[2] Патрисия Дж. Уильямс (Patricia J. Williams) «The protect Alberto Gonzales Act of 2007» (Акт о защите Альберто Гонсалеса 2007 года), *Nation* от 27 августа 2007 года.

Но большинство коммуникаций все же остаются незашифрованными, и тайный враг – Ева или кто-то другой – не замедлит подключиться.

Сегодня люди не особенно беспокоятся о защите коммуникаций, не осталось и следа горячки, рождаемой «криптографическими войнами» всего десять лет назад. Футуристические предсказания обеих воюющих сторон оправдались. С одной стороны, технологии шифрования доступны всем, и люди могут скрыть содержимое своих сообщений, чего и боялось правительство (например, политики часто спекулируют на слухах о том, что террористическая организация Аль-Каида пользуется программой PGP).[1] В то же время развитие Интернета увеличивает возможности для наблюдения за пользователями, о чем предостерегали противники государственного контроля технологий шифрования.

Хотя сейчас противоправное запрещение гражданских средств шифрования и невозможно, равновесие социальных и системных аспектов прикладной криптографии неустойчиво. Приведет ли некая информационная катастрофа, связанная с потерей личных данных, к повсеместному переобучению пользователей Интернета или всеобщим регулятивным изменениям в корпоративных практиках? Предложит ли ведущий поставщик почтовых сервисов и программ автоматическое шифрование электронной почты как базовую услугу в ответ на беспокойство пользователей за свою информационную безопасность?

Итоговый вопрос повестки дня таков: когда автоматическое шифрование сообщений станет таким же привычным и незаметным, как шифрование коммерческих транзакций, перевесят ли преимущества возможности защиты персональной информации, свободы слова и личной свободы те трудности, которые возникнут в реальной защитной работе правоохранительных органов, утративших возможность подключения и прослушивания?

Независимо от будущего технологий шифрования коммуникаций у прикладной криптографии есть еще один аспект применения. Возможности абсолютно точного копирования цифровой информации и мгновенной связи со всем миром нанесли мощный удар по праву интеллектуальной собственности в виде миллионов копий фильмов и музыки, загружаемых подростками. Технологии шифрования позволяют обрабатывать видео- и аудиозаписи, чтобы воспроизвести их могли только определенные люди, – блокируя, таким образом, этот участок цифровой экспансии. Эволюция понятия авторского права – это следующая остановка на нашем путешествии по захваченной битами территории.

---

[1] *www.strategypage.com/dls/articles/2004 года.850.asp*

Глава 6 | Нарушение равновесия

Кому принадлежат биты?

Автоматизированное правосудие для автоматизированных преступлений

Декабрь 2005 года, штат Орегон, США. Таня Андерсен ужинала со своей восьмилетней дочерью, когда в дверь постучали. Это был судебный исполнитель, доставивший исковое заявление от Американской ассоциации звукозаписывающих компаний (Recording Industry Association of America, RIAA) – коммерческой организации, представляющей несколько звукозаписывающих компаний, которые совместно контролируют свыше 90% рынка звукозаписей в США. В заявлении ассоциации сообщалось, что мать-одиночка, живущая на социальное пособие, должна выплатить истцу около миллиона долларов за незаконное скачивание примерно 1200 звуковых дорожек в жанре «гангстерский рэп» и другой защищенной авторскими правами музыки.[1]

Дело мисс Андерсен началось за 9 месяцев до описанных событий с письма от некой юридической конторы из Лос-Анджелеса. В письме было сказано, что «несколько звукозаписывающих компаний» подали иск против женщины за нарушение авторских прав, и теперь она должна выплатить от четырех до пяти тысяч долларов или понести иное наказание. Мисс Андерсен посчитала письмо проделкой мошенников и написала протест в ассоциацию, заявляя, что никогда не скачивала музыкальные файлы. Женщина даже предложила представителям ассоциации проверить жесткий диск ее компьютера, но получила отказ. В какой-то момент представитель ассоциации сказал мисс Андер-

---

[1] Эшбел С. Грин (Ashbel S. Green) «Music Goliath unloads on wrong David» (Голиаф от индустрии музыки сражается не с тем Давидом), *The Oregonian* от 1 июля 2007 года. Больше подробностей можно найти в деле «Андерсен против Atlantic Recording Corporation и др.», (3:2007cv00934, окружной суд штата Орегон в Портленде, принято в делопроизводство 22 июня 2007 года), *www.ilrweb.com*.

сен, что верит в ее невиновность, однако ассоциация не бросит начатое дело, поскольку такой исход создаст нежелательный для звукозаписывающих компаний прецедент.

Огромное количество материалов по случаям, связанным с защитой авторских прав, можно найти на сайте *www.chillingeffects.org*. Это совместный проект Фонда электронной безопасности и нескольких университетских правовых организаций.

После декабрьских событий мисс Андерсен наняла адвоката и добилась от судьи решения о проверке компьютера. Собственный эксперт ассоциации звукозаписывающих компаний признал, что компьютер мисс Андерсен никогда не использовался для нелегального скачивания музыки. Но вместо того чтобы прекратить дело, ассоциация зашла еще дальше. Ее адвокат потребовал, чтобы дочь мисс Андерсен дала показания в суде. Ассоциация даже попыталась самостоятельно доставить девочку в суд: неизвестная женщина позвонила в школу и, представившись бабушкой, попыталась выяснить расписание занятий. Адвокаты ассоциации связывались с друзьями и родственниками мисс Андерсен, пытаясь представить женщину как криминальную личность, которая коллекционирует музыку, призывавшую к насилию и расизму. Давление на 41-летнюю мисс Андерсен, страдавшую от болезни и стресса, заставило женщину отказаться от программы реабилитации. Вместо этого мисс Андерсен потребовались услуги психологов. Наконец, спустя два года несчастная мать-одиночка вернулась к судебному делу и составила заявление, требовавшее предоставления ассоциацией доказательств по делу. Доказательств не нашлось, и суд закрыл дело. В настоящее время мисс Андерсен судится с ассоциацией по встречному иску о сфабрикованном обвинении.[1]

26 000 исков за 5 лет

Начиная с 2003 года ассоциация возбудила против граждан более 26 000 исков о нелегальном копировании.[2] Процесс начался, когда занимающаяся расследованиями и подотчетная ассоциации компания Media-Sentry подключилась к файлообменной сети для поиска компьютеров,

[1] Дженет Ньютон (Janet Newton) «RIAA named in first class action» (RIAA в списке коллективного заявления), *p2planet* от 16 августа 2007 года, *www.p2pnet.net/story/13077*.

[2] Джошуа Фрид (Joshua Freed) «RIAA:Expect More Music Download Suits» (RIAA: ожидается еще больше исков о скачивании музыки), *Lexisone* от 4 октября 2007 года, *www.lexisone.com/news/ap/ap100407e.html*.

распространяющих музыкальные файлы. При обнаружении подходящих файлов агент отправляет IP-адрес и список файлов в Группу по противодействию пиратству ассоциации звукозаписывающих компаний (RIAA Anti-Piracy group). Сотрудники группы скачивают и прослушивают файлы, чтобы убедиться, что это действительно звукозаписи, защищенные авторским правом. Затем ассоциация составляет иск против владельца компьютера, которому соответствует зафиксированный IP-адрес (объяснение понятия IP-адреса и других элементов структуры Интернета см. в приложении). Имя владельца компьютера выясняется путем судебного запроса к интернет-провайдеру с приложением IP-адреса. Ассоциация посылает на имя пользователя письмо с указанием списка файлов музыкальных композиций и предложением возместить ущерб, обычно оцениваемый примерно в 4000 долларов. Для ускорения оплаты даже создан веб-сайт *p2plawsuits.com*.[1]

Так в цифровом веке выглядит автоматизированная форма правосудия, предназначенная для автоматизированных преступлений. Файлообменные программы обычно сконфигурированы так, чтобы запускаться и выполнять обмен файлами без особого участия человека. Обмен происходит в фоновом режиме и обычно не требует пользовательской настройки.

Автоматизированная форма правосудия не свободна от ошибок. Соответствие имени и IP-адреса не является строго однозначным – в одной беспроводной сети, например, несколько компьютеров могут совместно использовать один IP-адрес. Интернет-провайдер, распределяющий IP-адреса, может менять их, так что IP-адрес компьютера, предоставляющего файлы для обмена, в другое время может быть назначен совсем к другому компьютеру. Если компьютер все-таки тот же, то может быть невозможным установить личность пользователя, инициировавшего файловый обмен. Кроме того, возможны сбои и ошибки в отчетах.

Руководство ассоциации понимает, что в процессе есть изъяны, но не видит другого способа остановить нелегальное скачивание музыки. Дело не только в фактически бесплатном распространении продуктов ассоциации, но и в возможности исков со стороны исполнителей, которые в принципе могут подать свои иски к ассоциации за неисполнение обязанностей по защите прав самих исполнителей. Эми Вайс, старший вице-президент ассоциации по связям, поясняет: «Когда ловишь рыбу сетью, в сеть иногда попадаются и дельфины... Но мы понимаем и то,

---

[1] Рэй Бекерман (Ray Beckerman) «How the RIAA Litigation Process Works» (Как работает процесс преследования от RIAA), *info.riaalawsuits.us/howriaa_printable.htm*. Также см. заявление Карлоса Линареса о правовом преследовании нарушителей авторских прав, окружной суд штата Массачусетс, дело 1:07-cv-10834-NG, принято в производство 2 мая 2007 года, *www.ilrweb.com*.

что это «киберворовство» необходимо остановить».[1] Кроме мисс Андерсен «дельфинами» оказались: семья из штата Джорджия, в которой вовсе не было компьютера; парализованный житель штата Флорида, якобы скачавший файлы в штате Мичиган; старушка из Западной Вирджинии, которая, во-первых, ненавидела компьютеры, а во-вторых, давно скончалась.[2]

Правонарушение вам дорого обойдется

Ошибочно или нет, но большинство людей, получающих письма от ассоциации, предпочитают заплатить. Стоимость судебных расходов намного превысит сумму штрафа, особенно при проигрыше дела: за каждый скачанный файл правонарушителю придется заплатить не менее 750 долларов. Проигрыватель iPod с диском емкостью 20 гигабайт (1 гигабайт – это примерно миллион байт) вмещает 4000 композиций. Нелегальное скачивание такого количества файлов может обойтись в 3 млн долларов – легальная покупка файлов на сервисе iTunes обойдется в тысячу раз дешевле.

750 долларов за композицию

Минимальное взыскание с нарушителей авторских прав, *устанавливаемое судом*, составляет 750 долларов за каждый факт нарушения прав. В случаях, когда может быть установлено явно умышленное нарушение авторских прав, суд может назначить возмещение ущерба вплоть до 150 000 долларов за факт, или 600 000 000 за содержимое проигрывателя iPod. Если защитник сможет доказать отсутствие злого умысла, суд все равно *должен* назначить возмещение ущерба не менее, чем 200 долларов за факт – «всего лишь» 800 000 долларов за 4000 композиций.[3]

---

[1] Цитируется в статье Денниса Родди (Dennis Roddy) «The Song Remains the Same» (Композиция остается все той же), питсбургская *Post-Gazette* от 14 сентября 2003 года, *www.post-gazette.com*.

[2] Лоуэлл Викерс (Lowell Vickers) «Family sued by recording industry» (Индустрия звукозаписи преследует семью), *Rockmart Journal* от 24 апреля 2006 года, *news.mywebpal.com*. Также см. дело «Уолтер против Паладука», окружной суд Восточного Мичигана, описанное на странице «RIAA Sues Stroke Victim in Michigan» (RIAA возбуждает в Мичигане иск против парализованного), *recordingindustryvspeople.blogspot.com*. Также см. Эрик Бангеманн (Eric Bangemann) «I Sue Dead People» (Я подаю иски против умерших), *Ars Technica* от 4 февраля 2005 года, *arstechnica.com/news.ars/post/2005 года.0204-4587.html*.

[3] Кодекс законов США, том 17, раздел 504 (2007).

«Мы хотели дать понять»

В октябре 2007 года Джейми Томас из штата Миннесота, мать-одиночка с двумя детьми и доходом 36 000 долларов в год, была признана виновной в распространении 24 музыкальных композиций через файлообменную сеть Kazaa и оштрафована на 222 000 долларов – по 9250 за каждый файл. Это было первое из дел Американской ассоциации звукозаписывающих компаний, рассматриваемое судом присяжных. Ранее люди предпочитали заплатить или, как в случае Тани Андерсен, дело было прекращено или в иске было отказано. В соответствии с положениями законодательства штраф в этом случае мог составить от 18 000 до 3 600 000 долларов. Выступая перед прессой, один из присяжных сообщил, что в коллегии высказывалось мнение о назначении как верхней, так и нижней суммы штрафа: «Мы хотели дать понять, чтобы вы не делали ничего подобного и что мы вас предупредили».

Как сказал адвокат Ассоциации после прочтения, выслушав приговор: «Вот что может случиться, если вы не заплатите».[1]

Сетевое правосудие, автоматизированное расследование автоматизированных правонарушений и 3 млн долларов за содержимое проигрывателя iPod – это потомки обитателей того, еще не оцифрованного, мира, усилившие свою мощь благодаря экспоненциально нарастающему вторжению битов. Плата за содержимое проигрывателя iPod, например, берет свое начало в Акте об авторских правах (Copyright Act) от 1976 года, установившего минимальное *взыскание* с нарушителей в 750 долларов за каждый факт нарушения прав.

Смысл таких высоких сумм – обеспечить наказание, достаточное для того, чтобы отбить у потенциальных правонарушителей всякую охоту к нелегальному копированию (даже если действительные убытки правообладателя невелики). Размер штрафов чудовищно возрастает в эпоху цифрового копирования, когда каждый факт копирования (закачка и выкладывание файлов) считается *отдельным* фактом правонарушения. Подобный метод исчисления ущерба казался адекватным в 1976 году, когда можно было сделать лишь несколько нелегальных копий, одну за другой. Но сумма штрафа достигает астрономических величин в условиях, когда за несколько часов по высокоскоростному соедине-

[1] Дэвид Кравиц (David Kravets) «RIAA Juror: 'We Wanted to Send a Message'» (Присяжные RIAA: «Мы хотели дать понять»), блог Wired, 9 октября 2007 года, *blog.wired.com/27bstroke6/2007/10/riaa-juror-we-w.html*.

нию на домашний компьютер можно загрузить несколько тысяч музыкальных композиций.

Цифровая экспансия сделала размер штрафа за нарушение авторских прав несоизмеримым с собственно ущербом от правонарушения, но не только: она также способствовала гораздо более фундаментальному изменению: почти полному пренебрежению правом на интеллектуальную собственность. До появления Интернета обычный человек не мог своими действиями причинить серьезный ущерб правообладателю. Допустим, некто создал 50 фотокопий книги и продал экземпляры на улице. Это, конечно, факт нарушения авторских прав. Но, во-первых, это требует значительного объема работы, а во-вторых, ущерб правообладателя невелик.

Пожалуй, одно из самых тяжелых последствий цифрового взрыва – потеря равновесия между правообладателями и пользователями.

Пожалуй, одно из самых тяжелых последствий цифрового взрыва – потеря равновесия между правообладателями и пользователями. Рядовые граждане получили возможность практически без усилий копировать и распространять огромные массивы информации. Слушатели вступают в борьбу с производителями музыки, прибыль которых зависит от того, следуют или нет обычные люди правовым нормам. Сегодня миллионы людей могут считаться «пиратами» или «ворами», а компаниям досталась роль противников инновационного развития и свободы потребительского выбора, пытающихся любыми средствами защитить свои устаревшие бизнес-модели.

Войне за авторские права на территории Интернета уже больше 15 лет. Технологии, раскручиваясь по спирали, помогают все большему числу людей распространять все больше данных. Движение спирали пытается сдержать законодательная инициатива правообладателей, предлагающих все новые законы со все более суровыми наказаниями. Порой закон даже пытается запретить новые технологии еще до их появления. Иски к матерям-одиночкам – это всего лишь второстепенные направления современной войны за ресурсы интеллектуальной собственности. Если не остановить гонку вооружений, к потерям завтрашнего дня добавятся свободный Интернет и инновационное развитие, которое питает информационную революцию.

Акт о противодействии электронному воровству: распространение цифровых копий – это преступление

Нарушение авторских прав в США не считалось преступлением до конца XIX века, хотя нарушитель мог быть призван к ответу за причинение ущерба. Впервые преступлением в отношении права на интеллекту-

альную собственность на почве получения выгоды был назван случай, произошедший в 1897 году. Максимальным наказанием за нарушение авторских прав стали год лишения свободы и штраф в 1000 долларов. Положение сохранялось до 1976 года, после которого Конгресс принял серию законов, последовательно увеличивавших меру наказания. Инициатива исходила главным образом от Американской ассоциации звукозаписывающих компаний и Американской ассоциации кинокомпаний (Motion Picture Association of America, MPAA). В 1992 году наказанием за нарушение авторских прав могло быть лишение свободы до десяти лет и немалый штраф, но только если нарушение было совершено «с целью получения коммерческой прибыли или личной финансовой выгоды». Без наличия коммерческих мотивов состава преступления не было.[1]

Положение дел изменилось в 1994 году.

В 1980-е Массачусетский технологический институт лидировал среди вузов по числу подключенных к Интернету компьютерных рабочих станций, доступных на территории студенческого городка. Даже в начале 1990-х доступные кластеры из мощных сетевых компьютеров были редкостью. В декабре 1993 года группа студентов обнаружила необычное поведение рабочей станции, которая не отвечала на запросы и выполняла интенсивные операции со своим жестким диском. Когда обслуживающий персонал исследовал этот «баг», то выяснилось, что станция выполняла функции файлового сервера и сетевой конференции – узла, на котором пользователи Интернета могли обмениваться файлами. Большинство файлов оказалось компьютерными играми; также было несколько программ для обработки текстов.

Как и большинство учебных заведений, институт предпочел бы провести внутреннее расследование событий, но этому не суждено было случиться: сведения об этой станции запросило ФБР. Агенты ФБР вели наблюдение за несколькими взломщиками программ из Дании, которые пытались использовать институтские компьютеры, чтобы получить доступ системам Национальной метеорологической службы (National Weather Service). Измерив входящий и исходящий потоки данных, ФБР заметило необычную активность отдельной станции института. Приложение сетевой конференции не имело отношения к операции ФБР, но руководство института решило доверить ему расследование событий. Сотрудник ФБР исследовал компьютер и выяснил имя виновного студента.

---

[1] Более детальное обсуждение усиления мер наказания вплоть до 1999 года см. в публикации Лидии Пэлас Лорен (Lidia Pallas Loren) «Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement» (Дигитализация, коммодизация, криминализация: эволюция преступного нарушения авторских прав и важность наличия умысла), *Washington University Law Quarterly*, 77:835, 1999.

Департамент юстиции (Justice Department) взялся за дело. В 1994 году индустрия программного обеспечения быстро набирала обороты, а Интернет только готовился предстать перед взорами общественности. И уже существовала сила, позднее получившая название «компьютерного пиратства». В своем заявлении прокурор округа Бостон сообщал, что сетевая конференция, установленная на рабочей станции института, нанесла ущерб на сумму больше миллиона долларов[1], и добавлял: «Мы должны достойно ответить культуре, которая считает, что никто не пострадает из-за этих фактов воровства и что нет ничего плохого в пиратском копировании программного обеспечения».

То, что произошло в институте, строго говоря, является нарушением авторских прав, но действия виновного не были нацелены на получение личной выгоды: нет состава преступления – нет оснований для действий Департамента юстиции. Здесь можно было бы усмотреть основания для гражданского дела, но компании, чье программное обеспечение было незаконно скопировано, не были заинтересованы в подаче иска. После обращения к вышестоящим инстанциям в Вашингтоне прокуратура Бостона возбудила против студента дело о мошенничестве на основании того, что он способствовал переправке за границу краденого имущества (программ).

На судебном заседании федеральный окружной судья Стернс отклонил заявление прокуратуры, сославшись на решение Верховного суда о том, что нелегальные копии не могут считаться краденым имуществом. Судья Стернс сделал выговор студенту, описав его поведение как «небрежное и безответственное». Судья также предложил, чтобы Конгресс изменил законодательство об авторском праве, сделав возможным уголовное расследование подобных дел по мере необходимости. При этом судья сделал акцент на том, чтобы именно Конгресс, а не суды, сказал последнее слово. Чтобы принять адекватное решение о наказаниях, придется «криминализировать поведение... мириадов пользователей домашних компьютеров, поддавшихся искушению скопировать хотя бы одну программу для персонального использования». Судья цитировал показания в Конгрессе разработчиков программного обеспечения о том, что даже они не могут считать такой исход желательным.[2]

В 1997 году Конгресс сказал свое слово, приняв Акт о противодействии электронному воровству (No Electronic Theft Act, NET Act). Описанный сторонниками как «перекрывающий тайные ходы» (подобные установленной на компьютере Массачусетского технологического института программе сетевой конференции), Акт сделал возможным уголовное преследование любого случая незаконного копирования материалов стоимостью выше 1000 долларов вне зависимости от мотивов.

---

[1] Джош Хартманн (Josh Hartmann) «Student Indicted on Piracy Charges» (Студент обвиняется в пиратстве), *The Tech* от 8 апреля 1994 года, *the-tech.mit.edu/V114/N19/piracy.19n.html*.

[2] Окружной суд штата Массачусетс, 871 F. Supp. 535, 28 декабря 1994.

Это был ответ на предложение судьи Стернса, хотя и без учета его предупреждения: копирование на персональный компьютер даже одной дорогой компьютерной программы могло закончиться годом тюрьмы. Но Конгресс пошел еще дальше, приняв Акт о предупреждении цифрового пиратства и усовершенствовании мер по защите авторских прав 1999 года (Digital Theft Deterrence and Copyright Damages Improvement Act). Разработчики нового Акта считали, что предыдущего оказалось недостаточно для уничтожения пиратства, поэтому необходимо ужесточить наказания.[1] Гонка вооружений в войне за интеллектуальную собственность набирала обороты.

Технологический переворот: peer-to-peer

Акт о противодействии электронному воровству ознаменовал рубеж, начиная с которого Интернет стал зоной ответственности за нарушение авторских прав. И этот закон стал далеко не последним.

Летом 1999 года Шон Фэннинг, студент Северо-Восточного университета (Northeastern University), стал распространять свою новую программу для обмена файлами, основав компанию Napster вместе со своим дядей. Программа Napster обеспечивала легкий способ обмена файлами, особенно музыкальными композициями, через Интернет в невиданном масштабе.

Вот как работает система обмена: предположим, что пользователь Мэри хочет поделиться своей копией хита «Ангел» Сары Маклахлан. Мэри обращается в службу Napster, которая добавляет в свой каталог запись «АНГЕЛ; Сара Маклахлан» и идентификатор компьютера Мэри. Пользователь Бет прочитает содержимое каталога и найдет запись. После этого компьютер Бет напрямую подключается к компьютеру Мэри и скачивает файл без дальнейшего участия сервиса Napster. Подключение и скачивание выполняются автоматически при помощи установленной на обоих компьютерах программы Napster.

Ключевое отличие файлообменной системы от такого приложения, как сетевая конференция, состоит в том, что последняя является *централизованной системой*. В такой системе файлы сохраняются на центральном компьютере, откуда и осуществляется скачивание. В системе Napster есть только центральный каталог с указанием компьютеров, содержащих файлы. Отдельные компьютеры файлообменной сети подключаются друг к другу напрямую. Это называется архитектурой *peer-to-peer*[2] (*одноранговая*, *децентрализованная*, *пиринговая* архитектура).

---

[1] Выступление в Сенате сенатора Лихи (Leahy) от штата Вермонт, протокол от 12 июля 1999 года, S8252–S8254, *cyber.law.harvard.edu/openlaw/DVD/dmca/cr12jy99s.txt*.

[2] Peer-to-peer, P2P — буквально «от узла-к узлу». – *Прим. перев.*

Как можно понять из рис. 6.1, архитектура peer-to-peer позволяет более эффективно использовать ресурсы сети, чем централизованная архитектура. В последней пользователи (клиенты), желающие получить файлы, должны подключиться к одному центральному компьютеру (серверу).

С ростом числа одновременных подключений скорость скачивания для каждого пользователя понижается, иногда вплоть до остановки. В системе peer-to-peer сервер должен предоставить лишь немного данных из каталога, а нагрузка по передаче файлов распределяется между всеми пользователями.

Даже обычных для 1999 года медленных подключений оказалось достаточно для передачи миллионов файлов музыкальных композиций по сети Napster... что и происходило. К началу 2001 года в сети Napster было зарегистрировано 26 миллионов пользователей. В некоторых учебных заведениях более 80% потока данных внутри студенческого городка приходилось на сеть Napster. Студенты собирали Napster-вечеринки. Нужно было пригласить друзей, подключить к компьютеру звуковую систему и выйти в Интернет. У кого-нибудь из миллионов пользователей обязательно была желаемая мелодия или композиция. Это был неиссякаемый музыкальный рог изобилия; универсальная медиатека.

Наказание за соучастие

Радуя весь мир, эта медиатека не доставляла никакой радости медиаиндустрии. Предыдущие методы обмена файлами, обычно в небольших группах среди друзей, практически не были потерями с экономической точки зрения. Даже установленная на компьютере Массачусетского технологического института программа сетевой конференции обслуживала едва ли несколько сотен пользователей. Сеть Napster имела гораздо большие масштабы: каждый участник сети мог поделиться музыкой с несколькими сотнями тысяч «друзей». Индустрия звукозаписи немедленно забила тревогу, и в декабре 1999 года Американская ассоциация звукозаписывающих компаний подала иск к владельцам сети Napster на сумму больше 100 миллионов долларов.

Компания Napster заявила, что не несет ответственности. Прежде всего, компьютеры компании никогда не копировали никаких файлов. Компания всего лишь предоставляла сервис каталога. Как можно призвать компанию к ответственности за обычную публикацию сведений в Интернете? Это нарушение права на свободу слова. К несчастью для компании Napster, федеральный окружной суд штата Калифорния отклонил возражения и в июле 2000 года признал компанию виновной в соучастии посягательству на право интеллектуальной собственности (то есть в разрешении другим посягать на права и получении прибыли от действий нарушителей). Год спустя, после

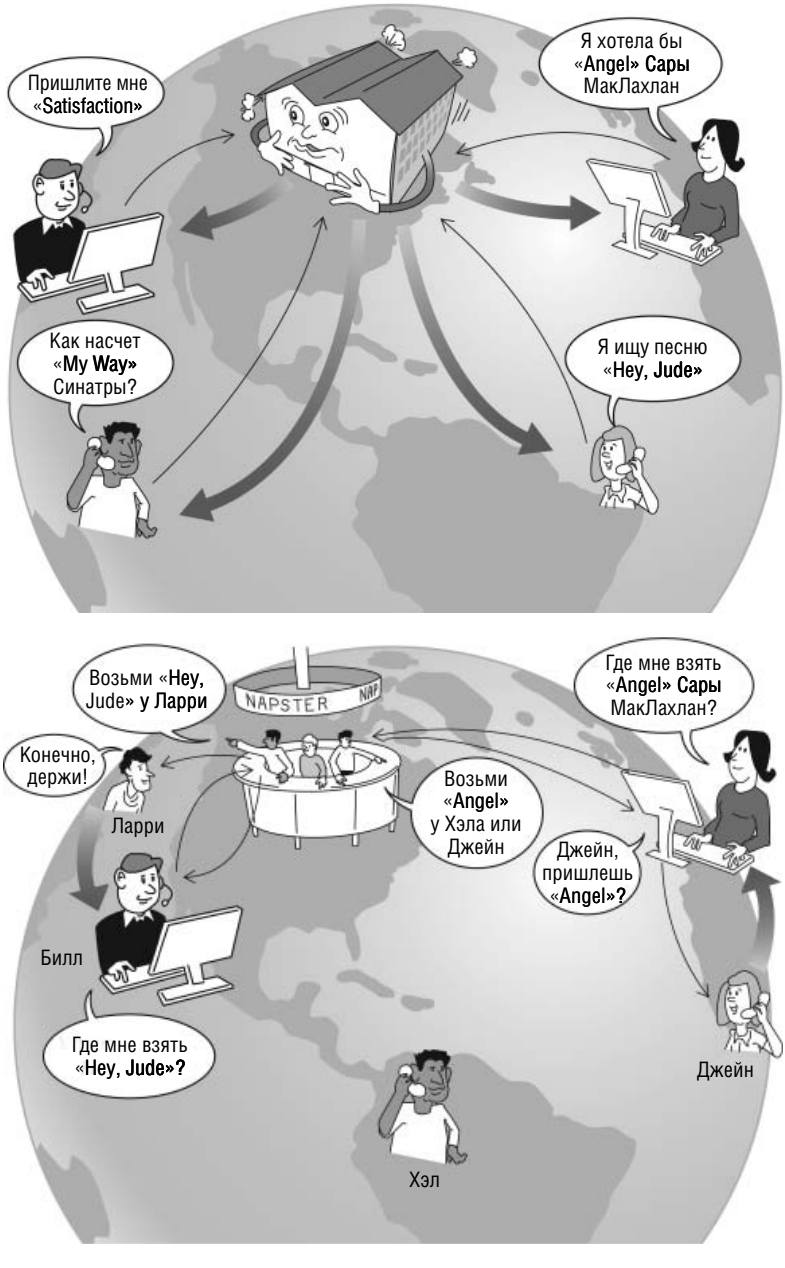


Рис. 6.1. *Схемы организации традиционной и пиринговой сетевых архитектур. Вверху: традиционная централизованная архитектура распространения файлов, когда клиенты скачивают файлы с центрального сервера. Внизу: пиринговая архитектура, такая как* ***Napster****, в которой сервер должен предоставить лишь немного данных из каталога, а передача файлов осуществляется между пользователями без участия сервера*

безуспешной апелляции, суд постановил закрыть файлообменный сервис Napster.[1]

Соучастие в нарушении прав собственности

Различаются два способа соучастия: *пособничество* – то есть, как в данном случае, намеренное предоставление средств, обеспечивающих совершение правонарушения, и *попустительство* – то есть получение выгоды от действий других при возможности предотвратить совершение правонарушения и отсутствии попыток это сделать. Компания Napster была признана виновной в обоих видах соучастия.

Сеть Napster исчезла, но запомнилась техническому сообществу как яркий пример эффективного использования децентрализованной природы Интернета. Не существует центрального компьютера, контролирующего Интернет; каждый компьютер в равной степени имеет возможность отправить другому компьютеру в Интернете сообщение. Подключенные к Интернету компьютеры на техническом жаргоне называются *узлами* (*peers*). Понимание природы Интернета как сети из равноправных узлов, напрямую взаимодействующих друг с другом – в противовес сети, в которой клиентские компьютеры обслуживаются центральным сервером, – отнюдь не является новым. Даже первичные спецификации Интернета, опубликованные в 1969 году, описывали новую сеть как сеть из узлов (хотя и в других терминах). Системы, объединяющие суперкомпьютеры в пиринговую сеть, использовались еще в начале 1980-х.[2]

Сеть Napster показала, что сеть, объединяющая миллионы узлов-персональных компьютеров обычных пользователей, основана на тех же принципах. Работа сети Napster нарушала закон, но продемонстрировала потенциал идеи. Немедленно стартовали разработка и внедрение распределенных вычислений. В 2000-2001 годах более 500 миллионов

---

[1] В этой истории полно манипуляций и ухищрений с законом. Даже после объявления банкротства и продажи активов компания Napster все еще существует в виде сервиса продажи файлов звукозаписей. Полное описание рождения и выживания компании Napster можно найти на странице Стефани Хорнунг (Stephanie Hornung) «Napster: The Life and Death of a P2P Innovator» (Napster: жизнь и смерть инноватора пиринговых сетей), *Berkeley Intellectual Property Weblog*, 15 января 2003 года, *journalism.berkeley.edu/projects/biplog/archive/000428.html*.

[2] Стив Крокер (Steve Crocker) «Host Software» (Узловое программное обеспечение), RFC № 1 к группе по обеспечению работы Интернета от 7 апреля 1969 года, *www.apps.ietf.org/rfc/rfc1.html*.

долларов были вложены в компании, занимающиеся разработкой приложений для пиринговых сетей. Из недр технической культуры обозначение «P2P» перешло в словарь техно-поп-культуры как общее название организаций всех типов – включая общественные, политические и корпоративные, – которые объединяет мощь несметного числа взаимодействующих индивидов, не опирающихся в своей работе на какие-либо центральные органы власти. Как было сказано в одном обзоре в 2001 году: «P2P – это образ мышления, а не отдельная технология или отрасль».[1]

Сеть Napster также позволила целому поколению пользователей ощутить вкус Интернета как универсальной медиатеки, за которую люди готовы отдать голоса. Звукозаписывающие компании, совместно боровшиеся против незаконного скачивания, не сумели объединиться и заполнить образовавшуюся в результате их усилий пустоту, создав законный и выгодный сервис сетевой музыки.

Вместо того чтобы постараться обратить файлообменные технологии себе на пользу, медиакомпании превратили технологии в угрозу своему бизнесу. Такой технологический консерватизм подогрел гонку вооружений, но и показал недальновидность медиакомпаний. Они уступили огромный сектор рынка более предприимчивым конкурентам. Через два года корпорация Apple запустила iTunes – первый коммерчески успешный сервис скачивания файлов музыкальных композиций.

Файловый обмен становится децентрализованным

В то же время начали рождаться новые файлообменные системы, основанные на других принципах, позволяющих обеспечить работу, избежав судебного преследования. «Ахиллесовой пятой» сети Napster был ее центральный каталог. Как постановил суд, управление каталогом означало управление файлообменной активностью, поэтому компания Napster должна была понести ответственность за нелегальный обмен файлами.

Новые системы полностью отказались от центральных каталогов. Одна из простейших файлообменных систем без общего каталога, называемая *flooding* (*лавинная рассылка*, *флудинг*) работает примерно так: каждый компьютер в файлообменной сети содержит список других компьютеров. Когда пользователь Бет хочет получить копию композиции «Ангел», компьютер Бет опрашивает все компьютеры в списке. Если композиция находится, то один или несколько компьютеров пересы-

[1] Клей Ширки, Келли Трюлов, Раил Дорнфест, Лукас Гонз (Clay Shirky, Kelly Truelov, Rael Dornfest, and Lucas Gonze) «2001 P2P Networking Overview» (Обзор состояния P2P-сетей в 2001 году), O'Reilly, 2001 год. Оценка ожидаемых инвестиций в 500 млн долларов цитируется здесь: *www.oreilly.com/catalog/p2presearch/summary/index.html*.

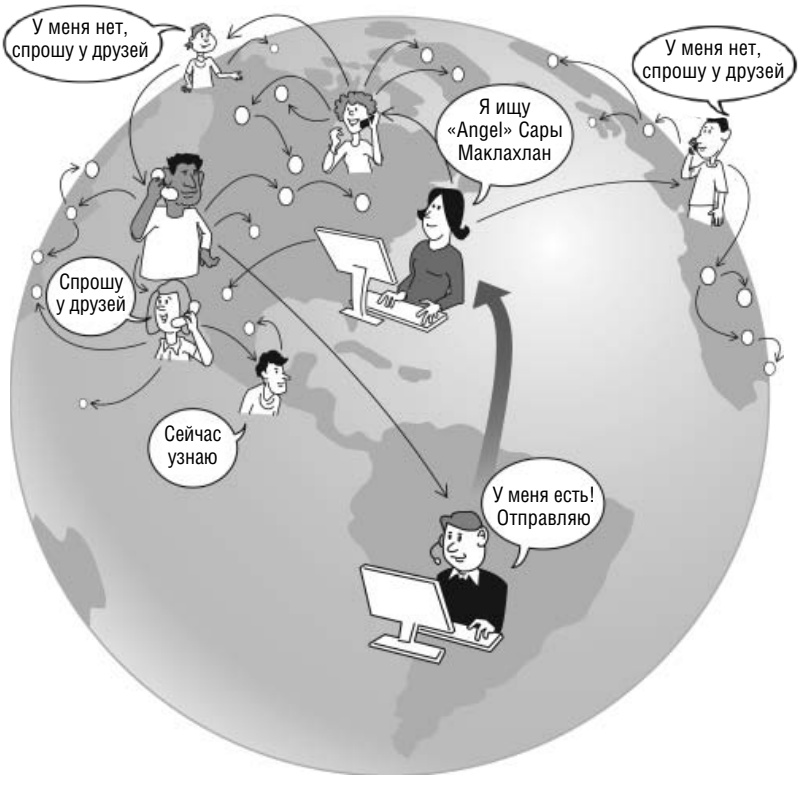


Рис. 6.2. *В отличие от* ***Napster-подобных систем, децентрализованные файлообменные системы,*** *вроде* ***Grokster, не используют центральные каталоги***

лают компьютеру Бет нужный файл, если нет, то каждый из компьютеров в списке Бет ретранслирует запрос компьютерам из собственного списка, и так далее, пока файл не найдется. Процесс показан на рис. 6.2.

В отличие от **Napster-подобной архитектуры, здесь нет общего каталога.** Такие распределенные архитектуры исключительно устойчивы. Сеть продолжает работать, даже если значительная часть компьютеров отключится или выйдет из строя, до тех пор пока остается достаточно узлов, чтобы ретранслировать запросы.

Сети с распределением содержания

Метод лавинной рассылки запросов в чистом виде слишком прост, чтобы обеспечить на практике существование достаточно больших сетей. Однако успех децентрализованных файлообмен-

ных систем стимулировал разработку *сетей с распределением содержания* (под «содержанием» подразумеваются файлы большого размера, которые возможно передавать потоком, например интернет-видео), наследующих эффективность и надежность технологий peer-to-peer.[1]

Правовая защищенность не гарантируется

Компании, разрабатывающие файлообменные системы нового поколения, надеются, что их распределенные архитектуры смогут защитить владельцев от судебного преследования за содействие нелегальному копированию. В конце концов, пользователи лишь получают от разработчиков программное обеспечение, а что они с ним делают – вне сферы контроля компаний. Так разве могут компании нести ответственность за действия пользователей? Напротив, для звукозаписывающей индустрии все это – вовращение сети Napster в новой ипостаси: злоупотребление свободой Интернета с целью массовых нарушений авторских прав.

В октябре 2001 года Американская ассоциация звукозаписывающих компаний подала иски против разработчиков трех наиболее популярных файлообменных систем – Grokster, Morpheus и Kazaa – о возмещении ущерба в 150 000 долларов за каждый факт нарушения авторских прав.[2]

Разработчики файлообменных систем возразили, что они не отвечают за действия пользователей. Кроме того, программное обеспечение разработчиков систем составляло только часть инфраструктуры файлового обмена. Если три компании-разработчика несут ответственность, то как насчет остальных? Как насчет корпорации Microsoft, чья операционная система позволяет пользователям копировать файлы? А компания Cisco, чьи маршрутизаторы ретранслируют нелицензионные копии? Несут ли ответственность производители компьютеров, на которых выполняются программы? Неужели законодательство против

---

[1] См., например, Хари Балакришан, М. Франс Каашок, Дэвид Каргер, Роберт Моррис, Йон Стоик (Hari Balakrishnan, M. Frans Kaashoek, David Karger, Robert Morris, and Ion Stoic) «Looking Up Data in P2P Systems» (Поиск данных в пиринговых системах), *Communications of the ACM*, февраль 2003 /VolT. . 46, № 2; также см. Стефанос Андруцелис-Феотокис Теотокис и Диомидис Спинеллис (Stephanos Androutsellis-Theotokis and Diomidis Spinellis) «A Survey of Peer-to-Peer Content Distribution Technologies» (Обзор пиринговых технологий распространения цифрового содержимого), *ACM Computing Surveys*, т. 36, № 4, декабрь 2004 года, с. 335–371.

[2] Иск MGM и др. против Grokster и др., *www.eff.org/IP/P2P/MGM_v_Grokster/20011002_mgm_v_grokster_complaint.pdf*.

файлообменного программного обеспечения возложит ответственность на всю компьютерную индустрию?

Верховный суд ответил на этот вопрос еще в 1984 году, рассматривая дело «Корпорация Sony против киностудии Universal Studios». Американская ассоциация кинокомпаний предъявила иск к корпорации Sony за продажу устройства, которое могло бы разрушить всю киноиндустрию, – видеомагнитофона с возможностью записи. Как заявил председатель ассоциации членам Конгресса в 1982 году: «А я говорю, что видеомагнитофон для киностудий и общества Америки – то же, что „бостонский душитель“ для одинокой домохозяйки».[1]

Голосованием пяти членов против четырех Верховный суд принял сторону корпорации Sony, постановив, что несмотря на распространение нелегального копирования с помощью видеомагнитофонов,

> ...продажа оборудования для копирования, равно как и продажа других товаров, не является нарушением закона, если товар главным образом используется для правомерных некоммерческих целей. Просто его следует использовать исключительно в законных целях.[2]

Разработчики высокотехнологичных продуктов рукоплескали. У них появился четкий критерий, который можно было использовать при оценке риска появления нового продукта на рынке. Указание на использование продукта «исключительно в законных целях» могло обеспечить разработчикам надежную защиту от правового преследования за содействие нелегальному копированию.

Сценарий 1984 года – новая технология угрожает существованию обкатанной бизнес-модели – повторился в 2001 году в деле разработчиков сети Grokster. Разработчики немедленно принялись в свою защиту цитировать решение по делу корпорации Sony, упирая на преобладание случаев правомерного использования файлообменных технологий.

В апреле 2003 года центральный федеральный окружной суд штата Калифорния согласился, что этот случай отличается от дела компании Napster, и отклонил иск, заметив, что Ассоциация звукозаписывающих компаний просила суд «выйти за строго очерченные границы существующего законодательства в области авторских прав».[3] В ответ Ассоциация начала охоту за отдельными пользователями файлообмен-

---

[1] Выступление председателя Ассоциации киностудий Джека Валенти (Jack Valenti) на слушаниях по теме «Home Recording of Copyrighted Works» (Копирование в домашних условиях произведений, защищенных авторскими правами) перед Подкомитетом по судам, гражданским свободам и отправлению правосудия Комитета по судоустройству в Палате представителей, 12 апреля 1982, *cryptome.org/hrcw-hear.htm*.

[2] Дело «Sony of America против Universal City Studios», 464 U. S. 417 (1984).

[3] Председатель окружного суда Стивен Уилсон, *www.eff.org/IP/P2P/MGM_v_Grokster/030425_order_on_motions.pdf*.

ных сервисов, жертвами которой стали, в частности, матери-одиночки Таня Андерсен и Джейми Томас.[1]

Постановление окружного суда было безуспешно обжаловано в апелляционном суде, том же самом, по решению которого тремя годами раньше должна была закрыться компания Napster:

> Подводя итог на основании представленных доказательств, окружной суд совершенно правильно вынес заключение, что указанное программное обеспечение предназначалось исключительно для легальных действий, и, таким образом, применил прецедент Sony–Betamax.[2]

Ассоциация звукозаписывающих компаний повторно апеллировала, и, когда Верховный суд согласился пересмотреть решение, весь сетевой мир затаил дыхание. Получат ли медиакомпании правовую защиту против масштабного нелегального обмена файлами? Будет ли сломлена защита разработчиков, построенная корпорацией Sony? В июне 2005 года суд вынес единогласное решение в пользу Ассоциации:

> Нами постановлено, что тот, кто распространяет устройство с целью способствовать нарушению авторских прав, что является ясно выраженным или на что указывают иные подтверждающие действия, предпринятые с целью способствовать нарушениям, несет ответственность за окончательные действия, нарушающие авторские права, со стороны третьих лиц.[3]

Вопрос намерения

Медиаиндустрия выиграла, хотя и с меньшими результатами, чем ожидала. Американская ассоциация кинокомпаний надеялась, что Верховный суд ужесточит формулировку «исключительно в законных целях», существовавшую со времен иска к корпорации Sony. Однако суд заявил, что ссылка на дело корпорации Sony в данном случае применена неверно, следовательно, нет необходимости изменять определение. Как сообщил суд, ответственность файлообменных компаний исходит не из возможностей программного обеспечения, но из целей его распространения.

Разработчики высокотехнологичных продуктов (не участники судебного процесса, которые уже выбыли из бизнеса) вздохнули было с облегчением от того, что успех корпорации Sony остался нетронутым.

---

[1] Новостной выпуск Ассоциации звукозаписывающих компаний (RIAA) «Recording Industry to Begin Collecting Evidence and Preparing Lawsuits Against File» (Звукозаписывающая индустрия начинает сбор доказательств и подготовку исков о незаконном копировании файлов) от 25 июня 2003 года, *riaa.com*.

[2] *www.eff.org/IP/P2P/MGM_v_Grokster/20040819_mgm_v_grokster_decision.pdf*

[3] Дело «MGM Studios против Grokster», 545 U. S. 913 (2005).

Но эти мысли быстро сменились другими. Решение по делу компании Grokster и других создало новый набор оснований, по которым компании или частные лица могли быть обвинены в соучастии в нарушении авторских прав. Как постановил Верховный суд: «Ничто из дела корпорации Sony не может привести суд к игнорированию доказательств умышленного содействия правонарушению, если таковые доказательства имеются».

О каких же доказательствах речь? Если кто-то обвиняет вашу компанию в соучастии правонарушению, то как вы сможете убедительно доказать, что в ваших действиях не было злого умысла? Похоже, корпорация Sony больше не может вас защитить.

Приведем пример: постановление по делу компании Grokster и других содержало основание «рекомендовалось для нелегального использования» как доказательство активных действий, предпринятых для соучастия в правонарушении. Корпорация Apple в 2001 году представила пакет приложений iTunes, содержащий модуль для копирования содержимого компакт-дисков, под рекламным слоганом «Rip, Mix, Burn» (Копируй, микшируй, записывай). Отразился ли здесь злой умысел корпорации Apple? Так думают многие, в том числе директор корпорации Walt Disney, заявивший перед Конгрессом в 2002 году: «Есть компьютерные компании, рекламные объявления которых на всю страницу, на всех досках объявлений от Сан-Франциско до Лос-Анджелеса говорят – как там у них? – «копируй, микшируй, записывай» детям, чтобы им купили компьютер».[1]

Нельзя пропускать рекламу

В 2001 году компания ReplayTV Network представила цифровой видеомагнитофон с функцией автоматической приостановки записи во время рекламных пауз. Также можно было копировать записи с одного магнитофона ReplayTV на другой. Ведущие кинокомпании и телевизионные каналы вчинили компании иск о соучастии в правонарушении. Компания обанкротилась еще до окончания слушаний. Ее имущество купил другой производитель, пообещавший не встраивать подобные функции в новые модели.[2]

---

[1] Из выступления генерального директора компании Walt Disney Майкла Эйснера (Michael Eisner) на слушаниях по теме «Защита произведений в цифровую эпоху» перед сенатским Комитетом по торговле, науке и транспорту 28 февраля 2002 года.

[2] Фред фон Ломан и Уэнди Зельцер (Fred von Lohmann and Wendy Seltzer) «Death by DMCA» (Уничтожены DMCA), *IEEE Spectrum Online*, июнь 2006 года, *www.spectrum.ieee.org/jun06/3673*.

Может ли ваша компания позволить себе подобный слоган после дела компании Grokster и других? Вы, конечно, можете рассчитывать, что выиграете в суде любое дело, но риск проигрыша может обернуться катастрофой. В отдельных случаях частных лиц, вроде Тани Андерсен, даже минимальное возмещение ущерба в 750 долларов за одну композицию может составить непосильную сумму в миллионы долларов за все (возможно, ложно приписанные) файлы.

Но компании-производители высокотехнологичных устройств могут в принципе понести ответственность за *каждую* нелегальную копию файла на *каждом* проданном устройстве. Допустим, вы продали 14 миллионов проигрывателей iPod (столько корпорация Apple продала в 2006 году), на каждом из которых находится 100 нелегальных копий; по 750 долларов возмещения ущерба за каждую копию составит более триллиона долларов! Эта сумма в сто раз превышает *общую* сумму продаж медиаиндустрии в 2006 году.[1] Подобная трактовка ответственности может показаться насмешкой, но таков закон. Это значит, что неверное решение может погубить компанию. Лучше быть консервативным и не выпускать продукцию, свойства которой могут стать поводом для судебного дела, даже если вы обоснованно уверены в их легальности.

Можно только догадываться о товарах и их функциях, недоступных сегодня из-за неопределенности понятия «злого умысла» и возможности кошмарных штрафов за «соучастие в правонарушении». Компании весьма неохотно показывают пример, хотя кто-то и может спросить, почему музыкальные файлы, распространяемые по беспроводному соединению с помощью проигрывателя Microsoft Zune, самоуничтожаются после трехкратного воспроизведения или почему видеомагнитофоны Tivo не оснащаются функцией автоматического пропуска рекламы или возможностью переноса записей на компьютер. Неслучайно генеральный директор некой крупной сети кабельного вещания в 2002 году назвал пропуск ТВ-рекламы воровством, хотя и уточнил, что посещать уборную допускается.[2]

Но предполагать только возможную ответственность довольно бессмысленно, поскольку риск ответственности не увеличивался в вакууме. В войне за авторские права открылся второй фронт. Оружием стали не только иски, но и технологии.

---

[1] Около 33,6 млрд долларов в 2006 году, *news.bbc.co.uk/2/hi/entertainment/4639066.stm*.

[2] Генеральный директор Turner Broadcasting System Джейми Келлнер (Jamie Kellner), интервью для *Cableworld*, 29 апреля 2002 года, *www.2600.com/news/050102-files/jamie-kellner.txt*.

Использовать только с разрешения

Компьютеры обрабатывают информацию путем копирования битов: между диском и оперативной памятью, между оперативной памятью и сетью, из одной области памяти в другую. В действительности, большинство компьютеров могут хранить биты в памяти только путем многократного (тысячи раз в секунду) повторного копирования. (Компьютеры распространенных типов используют такие устройства, как **DRAM, Dynamic Random Access Memory – динамическая память** с произвольным доступом. Слово «динамическая» как раз и указывает на многократное повторное копирование.) Соотношение этого типа копирования с тем, которое защищается авторским правом, – предмет серьезных интеллектуальных усилий профессоров права, а также адвокатов, ищущих новые основания для предъявления исков.

Компьютер не может запустить программу с диска без копирования программного кода в оперативную память. Такое копирование закон разрешает. Но предположим, что некто хочет просто *просмотреть* код в памяти, не запуская программу. Требуется ли для этого явное разрешение правообладателя? В 1993 году Федеральный апелляционный суд постановил, что требуется.[1]

Продолжая рассуждения, вспомним, что компьютер не может отображать графику на экране без ее копирования в выделенную область памяти, называемую экранным буфером. Означает ли это, что, купив цифровое изображение, вы должны каждый раз перед просмотром получить разрешение правообладателя? Отчет Департамента торговли за 1995 год содержал ответ, что требуется не совсем именно это, но что почти каждое использование цифровой работы требует копирования, следовательно, необходимо разрешение правообладателя.[2]

---

[1] Дело «MAI Systems Corp. против Peak Computer, Inc.», 991 F.2d 511 (9th Cir. 1993). Строгая формулировка копирования, принятая судом, позднее была раскритикована правоведами, однако в последующем стала базой для рассмотрения аналогичных дел. С обсуждением можно ознакомиться здесь: Джозеф П. Лю (Joseph P. Liu) «Owning Digital Copies: Copyright Law and the Incidents of Copy Ownership» (Обладание цифровыми копиями: закон об авторском праве и инциденты собственности на копии), 42 Wm. & Mary L. Rev. 1245, 1255–78 (2001). Законодательство об интеллектуальной собственности было изменено в 1998 году, чтобы разрешить копирование кода в память с целью обслуживания или устранения ошибок (Кодекс законов США, том 17, 117).

[2] Брюс А. Леман (Bruce A. Lehman) «Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights» (Интеллектульная собственность и национальная информационная инфраструктура: отчет рабочей группы по праву интеллектуальной собственности), 1995 год, с. 64–66, *www.uspto.gov/web/offices/com/doc/ipnii/*.

Цифровые права и доверенные системы

Теоретики права могут спорить, устанавливает ли законодательство об интеллектуальной стобственности будущее типа «использовать только с разрешения» для цифровой информации. Ответ не имеет особенного значения, так как будущее уже наступает и ведет за собой технологии управления цифровыми правами и доверенные системы (trusted systems).

Основная идея довольно проста. Если компьютеры так легко копируют и передают информацию, не требуя разрешения, то необходимо *изменить компьютеры* так, чтобы копирование и передача информации без разрешения стали труднодостижимыми или невозможными. Этого нелегко достичь, возможно, это вовсе недостижимо для компьютеров без разрушения их функциональности как устройств общего назначения. Тем не менее, эта идея развивается.

Вот пример: представим себе некую компанию Fortress Publishers, продающую цифровые произведения через Интернет. Компания, конечно, хочет, чтобы произведения были доступны только тем, кто за них заплатил. Компания может ограничить доступ пользователей к своему сайту с помощью паролей. (Кстати, множество цифровых произведений в настоящее время продается подобным образом, например на сайтах Wall Street Digest или Safari Books Online.) Этот способ работает (или работал до недавнего времени) неплохо для определенного типа данных, но есть проблема. Как может компания Fortress Publishers предотвратить дальнейшее распространение произведений людьми, купившими их?

Fortress может, к примеру, предотвратить дальнейшее распространение произведений с помощью шифрования, так что произведения могут быть открыты только программами, подчиняющимися определенным правилам. Если Fortress продает PDF-документы, созданные в приложении Adobe Acrobat, то пакет Adobe LiveCycle Enterprise Suite позволит ей определять, могут ли люди, открывшие документ в программе Adobe Reader, напечатать, изменить или частично копировать его. Компания может даже добавить функцию «звонка домой» через Интернет, то есть в момент открытия документа компании передается IP-адрес компьютера, на котором это было сделано. Аналогично, если компания продает файлы музыкальных композиций для проигрывателя Windows Media Player, то с помощью функции «Управление лицензиями» можно ограничить число воспроизведений композиции, возможность копирования на переносное устройство или компакт-диск или срок хранения.[1] Можно добавить функцию подключения к веб-серверу Fortress Publishers при каждой попытке воспроизведения, так чтобы сервер мог проверить лицензию и при необходимости потребовать оплату.

---

[1] Это позволяют делать такие программы, как Adobe LiveCycle Enterprise Suite (*www.adobe.com/products/livecycle/*) или Windows Media Rights Manager 10.1.2 SDK (*msdn2.microsoft.com/en-us/library/bb649422.aspx*).

Собственно принцип распространения цифровых данных совместно с информацией по ограничению ее использования называется «управлением цифровыми правами» (digital rights management, DRM). Системы с поддержкой управления правами широко используются; для таких систем есть промышленные стандарты (называемые *языками описания прав* – rights expression languages), описывающие широкий спектр накладываемых ограничений.[1]

Шифрование и управление цифровыми правами

В главе 5 объяснялись понятия шифрования с открытым ключом и цифровой подписи – технологии, делающие возможным публичное распространение защищенных данных. Сообщения, которыми обмениваются стороны, могут быть не только текстом, но и музыкой, видеозаписями, иллюстрированными документами и чем угодно еще. Как гласит первый битовый коан, «все это – только биты». Таким образом, поставщики цифровых произведений могут быть применять технологии шифрования для контроля соблюдения прав на просмотр видеозаписей или прослушивание музыки.

Системы управления цифровыми правами могут выручить компанию Fortress Publishers, однако на практике этот подход часто дает сбои. Как может компания быть уверена, что люди используют именно те программы, которые поддерживают управление цифровыми правами? Шифрование может добавить уверенности, но, как показано в главе 5, взломщики часто и без особых усилий снимают защиту шифров; в частности, это регулярно происходит с форматами PDF и Windows Media.[2]

---

[1] Одна из таких систем – XrML (eXtensible rights Markup Language – Расширяемый язык разметки прав). Система основана на оригинальной разработке Xerox Palo Alto Research Center, впоследствии лицензирована Microsoft, *www.xrml.org*.

[2] См., например, статью «Microsoft Windows Media copy protection broken» (Защита от копирования в Microsoft Windows Media взломана), *informity* от 12 сентября 2006 года, *informitv.com/articles/2006/09/12/microsoftwindowsmedia/*. В статье цитируются слова представителя корпорации Microsoft: «Корпорация долго считала, что ни одна из систем DRM не является абсолютно надежной, – и нашим партнерам, предоставляющим цифровое содержимое, это тоже известно». Во Всемирной паутине доступны средства снятия защиты с формата PDF. Мы бы даже предоставили читателям ссылки, но наш издатель беспокоится о возможных нарушениях закона.

Еще проще: модифицировать средство просмотра документов или программу-проигрыватель для сохранения незащищенной копии файла, а затем сделать незащищенные копии доступными для каждого пользователя Интернета. Чтобы исключить возможность снятия защиты, компания может положиться на операционную систему, которая потребует сертификации каждой программы, используемой для манипуляции защищенными файлами. Перед запуском программы операционная система проверит ее сертификат, чтобы выяснить, является ли программа одобренной и не была ли она модифицирована.

Уже лучше. Однако опытный взломщик может изменить саму операционную систему, чтобы запускать непроверенные программы. Что делать в этом случае? Встроить в каждый компьютер микросхему, которая будет проверять при каждом запуске состояние операционной системы. Если система модифицирована, – компьютер не загрузится. Микросхема должна быть защищена так, чтобы любая попытка отключить ее делала компьютер неработоспособным.

Базовая технология защитных микросхем была разработана в 1980-х и проверена в нескольких исследовательских проектах, но только с 2006 года была готова для широкого внедрения в персональные компьютеры. Необходимая микросхема, названная Trusted Platform Module (TPM), разработана консорциумом Trusted Computing Group – объединением разработчиков компьютерных программ и оборудования, сформированным в 1999 году.[1]

Больше половины продаваемых сегодня компьютеров содержат чипы TPM. Популярные операционные системы, включая Microsoft Windows Vista и некоторые версии GNU/Linux, могут использовать чипы TPM для поддержания безопасности. Одно из применений чипов TPM – «доверенная загрузка» (trusted boot) – предотвращает загрузку модифицированной (например, вирусом) операционной системы. Другое – «опечатанное хранилище» (sealed storage) – позволяет шифровать файлы так, чтобы их можно было открыть только на определенном компьютере. В связи с современным распространением вирусов и состоянием интернет-безопасности определенно можно сказать, что технология TPM будет внедряться повсеместно. По одной из оценок индустрии, к 2009 году более 80 % мобильных компьютеров будут оснащены чипами TPM.[2]

---

[1] Веб-сайт разработчиков: *https://www.trustedcomputinggroup.org*. Название организации – Trusted Computing Platform Alliance, ее первые члены – Intel, Microsoft, HP, Compaq и IBM.

[2] Шейн Рау (Shane Rau) «IDC Executive Brief: The Trusted Computing Platform Emerges and Industry's First Comprehensive Approach to IT Security» (Краткое руководство IDC: появление платформы Trusted Computing и первый современный подход индустрии к информационной безопасности), февраль 2006 года, *https://www.trustedcomputinggroup.org/news/Industry_Data/IDC_448_Web.pdf*.

Контроль за пределами защиты авторских прав

Проблему компании Fortress Publishers можно решить объединением защищенных чипами TPM компьютеров и программных систем управления правами. Но следует ли нам радоваться этому?

С одной стороны, это решение дает компании возможности контроля продаваемых материалов, далеко превосходящие границы авторских прав. Когда мы покупаем книгу, то можем: читать ее, когда захотим и столько раз, сколько нужно; прочитать от корки до корки или бегло пролистать; одолжить другу; перепродать; копировать фрагмент для отзыва; передать в школьную библиотеку; открыть без того, чтобы книга подключилась к серверу продавца, чтобы доложить о том, что ее читают. Нам не нужны разрешения, чтобы сделать все это. Хотим ли мы, чтобы эти права были отняты у нас, когда книги станут компьютерными файлами? А как насчет звукозаписей? видеозаписей? программ? Хотим ли мы этого?

Теперь обратимся к другой стороне – спору между звукозаписывающими компаниями и слушателями. Защищенные чипами TPM компьютеры и системы управления правами, превратившись в стандарт для персональных компьютеров, могут быть применены и по другому назначению. Те же методы, которые в одной стране могут предотвратить воспроизведение нелицензионных записей, в другой стране могут быть использованы, чтобы запретить людям слушать альтернативные политические заявления и читать оппозиционные газеты. Разработчики систем защиты лицензионного содержимого создали эффективные средства контроля использования информации, но еще никто не разработал эффективных методов ограничения подобного контроля. Один из разработчиков систем безопасности предупредил: «Доверенные вычисления (trusted computing) означают, что третья сторона может гарантировать, что ваш компьютер не подчиняется вашим командам».[1]

Те же методы, которые в одной стране могут предотвратить воспроизведение нелицензионных записей, в другой стране могут быть использованы, чтобы запретить людям слушать альтернативные политические заявления и читать оппозиционные газеты.

Другая проблема с системами управления правами заключается в том, что у монополистов будет больше возможностей блокировать неудобные им технологии. Системы управления правами нацелены на создание операционных систем, которые будут запускать только сертифицированные приложения, чтобы исключить запуск вирусов

[1] Слова Лаки Грина (Lucky Green) на конференции по состоянию систем управления цифровыми правами в Беркли 28 февраля 2003 года воспроизведены на странице *www.law.berkeley.edu/institutes/bclt/drm/trans/drm-2-28-p2.htm*.

или модифицированных средств просмотра документов или воспроизведения мультимедийных файлов. Дальнейшее развитие идеи приведет к созданию отрасли, в которой никто не сможет выпустить на рынок новый программный проигрыватель без разрешения медиаиндустрии или распространять *какое-либо иное* приложение без регистрации и одобрения компаний Microsoft, HP или IBM. Компания-разработчик программного обеспечения, которая будет представлять конкурентноспособную угрозу правящим кругам – продавцам электронных изданий, поставщикам операционных систем или производителям компьютеров, – может внезапно встретиться с «затруднениями» в получении сертификата на свои продукты. Одной из причин быстрого развития информационных технологий всегда была открытость этой сферы деятельности: не нужно просить разрешения, чтобы представить обществу новые программы или устройства. Контроль цифровых прав может стать угрозой прогрессу.[1]

Третья проблема с системами управления правами – то, что во имя безопасности и защиты от вирусов можно легко развязать бесконечную «гонку вооружений» по блокированию технологий, в которой не будет победителей и которая не обеспечивает реальной выгоды для владельцев защищенных данных. Как только взломщики найдут способ обойти систему защиты, чтобы получить свободную копию, они смогут распространять копии – а они привыкли не жалеть на это времени и усилий.

Возьмем, к примеру, нелегальное копирование фильмов. Особо опытные взломщики могли бы модифицировать аппаратуру своих компьютеров, содержащую чипы TPM, потратив на это немало усилий. Также можно было бы пойти более легким путем: не трогая чипы TPM, установить видеомагнитофон вместо компьютерного монитора. Медиаиндустрия предусмотрела такую атаку: есть стандарт, который предписывает передавать видеопоток высокого разрешения между устройствами в зашифрованном виде.

Операционная система Windows Vista для этой цели использует подсистему Output Protection Management[2] и таким образом позволяет пользователям не беспокоиться о том, что кинокомпании наложат запрет на просмотр фильмов в высоком разрешении на персональных компьютерах. Даже такая схема защиты уязвима: можно установить перед монитором видеокамеру. Результат, конечно, будет невысокого

---

[1] Джонатан Зиттрейн (Jonathan Zittrain) в книге «The Future of the Internet and How to Stop It» (Будущее Интернета и как остановить это) приводит аргументы в пользу того, что устойчивости Интернета как «производящей платформы» угрожают блокировки, создаваемые компаниями якобы ради безопасности.

[2] Дэйв Марш (Dave Marsh) «Output Content Protection and Windows Vista» (Защита исходящего содержимого и Windows Vista), 27 апреля 2005 года, *www.microsoft.com/whdc/device/stream/output_protect.mspx*.

качества, но, будучи один раз оцифрованным, не ухудшится при распространении в Интернете.

Эта брешь в защите, называемая «аналоговой точкой уязвимости» (analog hole), весьма беспокоит продавцов медиаданных, так как для нее не существует каких-либо технологических способов защиты. Джоан Роулинг пыталась предотвратить нелегальное копирование книги «Гарри Поттер и Дары Смерти» путем запрета на продажу даже электронной версии. Запрет не смог препятствовать поклоннику серии (см. главу 2) просто сфотографировать все страницы и разместить фотокопии в Интернете до начала официальной продажи книги.

По мнению одного эксперта по компьютерной безопасности, «цифровые файлы не могут быть некопируемыми, так же как вода не может не быть мокрой».[1] Можно сказать определенно: подход к контролю за авторскими правами, подобный DRM, труден, утомителен и чреват неучтенными побочными эффектами. Эти трудности породили третий (вместе с правовой ответственностью и системами управления цифровыми правами) ответ растущему уровню копирования информации в Интернете – криминализацию технологий.

Запрещенная технология

Строки текста, следующие за этим абзацем, могут быть запрещены для воспроизведения в книге, продаваемой на территории США. Авторы пропустили четыре строки посередине, чтобы защитить себя и издательство. Полный текст представляет собой компьютерную программу, предназначенную для снятия защиты с видеосодержимого дисков DVD, написанную на языке программирования Perl. Публикация информации о способе снятия защиты и получения возможности копирования видеопотока подпадает под действие раздела 17 USC § 1201 – Акта о защите авторских прав в цифровую эпоху 1998 года (Digital Millennium Copyright Act, DMCA). В указанной части закона технология обхода защиты цифрового содержимого объявляется противоправной. Не надейтесь, что в этой книге вы найдете ссылку или какое-то иное указание на источник, содержащий недостающий фрагмент программы. Окружной суд Нью-Йорка в 2000 году постановил, что даже предоставление интернет-ссылки на исходный текст является нарушением акта; позже апелляционный суд поддержал решение окружного.[2]

---

[1] Брюс Шнайер (Bruce Schneier) «The Futility of Digital Copy Prevention» (Тщетность предотвращения цифрового копирования), *CRYPTO-GRAM* от 15 мая 2001, *www.schneier.com/crypto-gram-0105.html*.

[2] Дело «Universal City Studios, Inc. против Corley», 273 F.3d 429 (2d Cir. 2001). Решение можно прочитать здесь: *www.eff.org/IP/Video/MPAA_DVD_cases/20011128_ny_appeal_decision.html*.

```
s''$/=\\2048;while(<>){G=29;R=142;if((@a=unqT="C*",_)[20]&48){D=89;_unqb24.qT.@
. . . (пропущено 4 строки) . . .
)+=P+( F&E))for@a[128..$#a]\\}print+qT.@a}';s/[D-HO-U_]/\\$$&/g;s/q/pack+/g;eval
```

Положения акта не только запрещают людям печатать в своих книгах всякую белиберду. Акт объявляет противоправным целый класс технологий, запрещая их разработку, продажу, публикацию записей и даже их обсуждение. То, что Конгресс решился на подобный шаг, показывает степень тревоги и озабоченности той легкостью, с которой обходится защита систем управления цифровыми правами (DRM). В параграфе 1201 акта Конгресс объявляет об ответственности не только за нелегальное копирование, но и за сам факт взлома цифровой защиты (даже если последующего копирования не было). Если вы зайдете на веб-страницу, содержащую текст Библии, и взломаете шифр, чтобы прочесть Книгу Бытия, это не будет нарушением авторских прав, но ваши действия будут являться фактом обхода защиты. Обход защиты сам по себе назван противоправным деянием, и за него полагаются не менее строгие меры наказания, чем за нарушение авторских прав: выплата суммы ущерба, а иногда и лишение свободы. Конгресс намеренно разграничил факт обхода защиты и факт нарушения авторских прав. Альтернативные предложения о наказании за обход цифровой защиты, только если за этим последовало нелегальное копирование, были рассмотрены и отвергнуты сенаторами.[1]

Тем временем список запретов Акта о защите авторских прав в цифровую эпоху расширяется. Как указано в параграфе 1201(a)(2):

> Никто не вправе производить, импортировать, публично распространять или иным образом делать доступными любые технологии, продукты, услуги, устройства, компоненты или их составляющие, которые... главным образом созданы или спроектированы с целью обхода мер, направленных на защиту имущества, охраняемого авторскими правами.

Здесь закон переходит от регулирования поведения (обхода защиты) к регулированию собственно технологий. Это большой шаг вперед, но, как сказал один из разработчиков законопроекта: «Я продолжаю верить, что мы должны запретить производство устройств, главная цель разработки которых – обход цифровой защиты, потому что я не думаю, что наказание за использование таких устройств достаточно действенно. Таким образом, разрешение на свободное распространение

[1] Были отвергнуты следущие альтернативные законопроекты: «Digital Copyright Clarification and Technology Act of 1997» (Акт о прояснении цифровых прав и технологиях интеллектуальной собственности), сенатор Эшкрофт (Ashcroft), 105-е заседание Конгресса, и «Digital Era Copyright Enhancement Act» (Акт об усовершенствованиях права интеллектуальной собственности в цифровую эпоху), сенатор Буше (Boucher).

устройств, обходящих цифровую защиту, и наказание только за нецелевое их использование представляется мне едва ли разумным».[1]

В области безопасности есть большая разница между миром атомов и миром битов. Опубликовано немало инструкций о том, как взламывать механические замки или как изготовить универсальную отмычку, если в наличии имеется только ключ от одного из типовых замков.[2] Но если замок – это алгоритм шифрования цифрового содержимого, а за «дверью» находится фильм «Пираты Карибского моря», то правила игры меняются. Федеральное законодательство запрещает публикацию любых сведений о том, как устроен цифровой «замок».

Законодатели, возможно, не видят альтернативы, но они создали ужасную форму регулирования, которая начинается с немедленного сурового наказания, а затем воплощается в жизнь и дает поблажки в отдельных прецедентах. Необходимость смягчения мер наказания была очевидной уже при разработке чернового проекта Акта о защите авторских прав в цифровую эпоху. Текст акта все же содержит некоторые послабления. В том числе, разрешение правоохранительным органам взламывать защиту для целей расследования преступлений, а также разрешение некоммерческим библиотекам снимать защиту с публикаций, но только чтобы решить, стоит ли приобретать публикацию. Акт также предусматривает некоторые типы исследований технологий шифрования при определенных ограничениях. Осознавая, что нарастает необходимость новых послаблений, законодатели дали указания директору Библиотеки Конгресса регулярно (каждые три года) проводить слушания, чтобы по мере необходимости пересматривать существующие и предлагать новые исключения из наказаний.

К примеру, в ноябре 2006 года, после годичных слушаний, новое исключение позволило американцам снимать защиту с мобильного телефона, чтобы перейти на обслуживание другим оператором. Исключение нашло широкое применение девять месяцев спустя, когда корпорация Apple выпустила мобильный телефон iPhone, привязанный к сотовой сети AT&T. Пользователи потребовали свободы выбора оператора, тогда несколько компаний начали снимать защиту за определенную плату. Однако положения Акта о защите авторских прав в цифровую эпоху настолько запутанны, что, хотя снятие защиты с *вашего собственного* телефона легально, распространение программ для снятия защиты или даже *публикация* сведений о способе разблокировки могут оставаться противозаконными. На этом фоне компания AT&T угрожала судебным

[1] Письмо члена Палаты представителей Барни Фрэнка (Barney Frank) Хэлу Абельсону от 6 июля 1998 года.

[2] См., например, Мэтт Блейз (Matt Blaze) «Cryptology and physical security: Rights amplification in master-keyed mechanical locks» (Криптология и физическая безопасность: надежность прав в механических замках с мастер-ключами), *IEEE Security and Privacy*, март/апрель 2003 года, *www.crypto.com/papers/mk.pdf*.

преследованиям компаниям, предоставлявшим услуги разблокировки телефона iPhone.[1]

Защита авторских прав или боязнь конкуренции?

Положения Акта о защите авторских прав в цифровую эпоху плохо соотносятся с технологическими новшествами, поскольку страх наказания может остановить разработку нового устройства или программы. В условиях жесткой промышленной конкуренции всегда есть место искушению создать мощную систему запретов как основу для судебного преследования соперников по бизнесу.

В 2002 году компания-производитель гаражных ворот Chamberlain подала иск против производителя универсальных устройств для открывания ворот, мотивируя это тем, что универсальные трансмиттеры обходят защиту доступа при подаче радиосигнала на управление электроприводом ворот. После двух лет тяжбы дело заглохло в апелляционном суде.[2] В том же году корпорация Lexmark International судилась с производителем альтернативных картриджей, заявляя, что картриджи используют обход защиты, чтобы правильно функционировать в составе принтера.

Окружной суд признал иск обоснованным. Решение было успешно обжаловано в 2004 году[3], но в течение полутора лет альтернативные картриджи не могли появляться на рынке. В 2004 году корпорация Storage Technology успешно выиграла иск в окружном суде Бостона по поводу нарушения положений Акта о защите авторских прав в цифровую эпоху сторонними центрами технического обслуживания систем производства корпорации. Если бы апелляционный суд не отменил решение окружного, создалась бы ситуация, в которой ни одна независимая компания не смогла бы проводить техническое обслуживание компьютерного оборудования.[4] Это было бы примерно то же самое, как

---

[1] Дэвид Кравиц (David Kravitz) «Unlocking Your iPhone is Legal; Distributing the Hack, Maybe Not» (Разблокировка вашего iPhone – действие легальное; но разглашение техники разблокирования, возможно, нет), блог Wired, 27 августа 2007 года, *blog.wired.com/27bstroke6/2007/08/to-unlock-the-i.html*. Постановление директора Библиотеки Конгресса «Право на запрет обхода системы защиты авторских прав для технологий контроля доступа» от 27 ноября 2006 года, Федеральный реестр, т. 71, № 227. Правила и нормы, с. 68 472–68 480, *www.copyright.gov/fedreg/2006/71fr68472.html*.

[2] Дело «Чемберлен против Skylink», 381 F.3d 1178 (Fed. Cir. 2004). Иск подан в декабре 2002 года, *www.eff.org/legal/cases/Chamberlain_v_Skylink/MotionSummJudgment.pdf*.

[3] Дело «Lexmark International против Static Control Components», 387 F.3d 522 (6th Cir. 2004), *www.eff.org/legal/cases/Lexmark_v_Static_Control/2004 года.1026_Ruling.pdf*.

[4] Дело «Storage Technology Corp. против Custom Hardware Engineering & Consulting», 2005 год. U. S. App. LEXIS 18131, *fedcir.gov/opinions/04-1462.pdf*.

если бы автомобили марки Ford Taurus поставлялись с опечатанными капотами и ни один автомеханик, не имеющий лицензии корпорации Ford, не имел бы права проводить осмотр или ремонт.

Благодаря этой и другим подобным тяжбам Акт о защите авторских прав в цифровую эпоху прозвали «Digital Millennium Competition Avoidance» (Предотвращение конкуренции в цифровую эпоху). К счастью, ни одно из дел не было полностью однозначно решено, так как судьи указывали, что предмет рассмотрения не представлял собой нарушение авторских прав – едва ли Конгресс разрабатывал злополучный акт для гаражных ворот. Но в делах, где затрагивается авторское право, антиконкурентная сущность акта проявляется в полной мере.

Представьте, что в 1984 году Верховный суд, рассматривая иск против корпорации Sony, принял иное решение и признал корпорацию виновной в нарушении авторских прав при производстве и продаже видеомагнитофонов. Видеомагнитофоны исчезли бы с рынка? Едва ли – на них был спрос. Вероятнее всего, производители электроники пошли бы на сделку с киноиндустрией, предоставив ей частичный контроль функциональности видеомагнитофонов. Устройства стали бы более регулируемыми в соответствии с требованиями киноиндустрии. Новые функции должны были бы проходить тестирование, и ни одна функция, не одобренная ассоциацией киностудий, не прошла бы на рынок. Возможности устройств были бы под контролем поставщиков данных.

Именно таким представляется сейчас наш мир, когда дело касается защищенных авторским правом цифровых данных. Если компания производит продукт, обрабатывающий цифровую информацию, то руководству компании следует побеспокоиться о возможности нарушения авторских прав, даже без учета Акта о защите авторских прав в цифровую эпоху. Для беспокойства есть весьма серьезные основания, особенно после дела сети Grokster. Но предположим, что устройство не разрабатывалось с противоправными целями. Даже в этом случае, если цифровая информация защищена системой управления правами, производитель должен считаться с ее ограничениями. Иначе возможно применение устройства для обхода защиты, так что его производство будет считаться нелегальным. Ограничения, наложенные системой управления цифровыми правами, полностью зависят от воли поставщика информации. Установив ограничения, компания Fortress Publishers сможет диктовать свою волю производителю любого устройства, которое обрабатывает защищенные данные, принадлежащие компании.

В случае с дисками DVD защиту выполняет алгоритм CSS, разработанный компаниями Matsushita и Toshiba и представленный в 1996 году. Как упоминалось в главе 5, алгоритм был в скором времени взломан – классический пример нарушения принципа Керкхоффса – и нелегальные программы для обхода защиты в настоящее время доступны в Интернете. Приведенные выше в этой главе и подвергнутые цензуре строки программного кода – одна из таких программ.

Хотя алгоритм CSS бесполезен для реальной защиты от копирования, он неоценим в качестве средства монопольной регуляции технологий. Любая компания, которая выпускает на рынок продукт, декодирующий содержимое дисков DVD, должна получить лицензию у основанной в 1999 году Ассоциации по контролю за копированием DVD (DVD Copy Control Association, DVD CCA).[1] Условия лицензирования полностью определяются желаниями руководства Ассоциации. Например, все проигрыватели дисков DVD должны поддерживать так называемый регион (region coding), который можно изменять, но не более пяти раз. «Регионы» не имеют никакого отношения к авторскому праву. Они нужны для поддержки маркетинговой политики киноиндустрии по выпуску фильмов в разных регионах мира в разное время. Среди лицензионных ограничений есть и такие, о которых можно узнать только после заключения лицензионного договора.

Лицо монополизированной технологии

Представьте, что вы работаете в компании, имеющей передовую идею по созданию устройства для работы с дисками DVD. Это может быть, к примеру, домашний кинотеатр с функцией копирования и сохранения содержимого дисков DVD для дальнейшего просмотра. И вы ищете способ, как это реализовать без нарушения авторского права. Ваша предполагаемая разработка востребована на рынке. В 2004 году начинающей калифорнийской компании Kaleidescape, разработавшей нечто подобное, пришлось защищаться от иска Ассоциации по контролю за копированием DVD. Основанием для иска стало нарушение лицензии CSS, по которой DVD-проигрыватели должны были работать только при наличии физического диска. В марте 2007 года суд штата Калифорния решил вопрос в пользу компании Kaleidescape на том основании, что положения лицензии были недостаточно четко сформулированы.[2] Однако решение было обжаловано. В любом случае, Ассоциация может в любой момент переписать лицензию. Судебные прения держали компанию Kaleidescape в напряжении в течение трех лет. Другая молодая компания, работавшая над аналогичным проектом, закрылась после того, как ей отказали в размещении венчурных фондов «вследствие возможной угрозы правового преследования со стороны Ассоциации по контролю за копированием DVD».

Ограничение лицензирования технологии DVD началось с 2000 года. Похожим образом дело обстояло и с высококачественным кабельным телевидением. Кампания по расширению монопольности всех потребительских медиатехнологий лоббируется в Вашингтоне под флагом

---

[1] *www.dvdcca.org/*

[2] Рик Мерритт (Rick Merritt), «Judge rules against DVD consortium», (Судья вынес решение не в пользу консорциума DVD»), *EE Times*, 29 марта 2007 года. *www.eetimes.com/news/latest/showArticle.jhtml?articleID=198701186*.

передовой инициативы. Все больше пробных шаров запускается во имя защиты авторских прав. Для рассмотрения Конгрессу был предложен билль о запрете записи в домашних условиях спутникового радио. Крупнейшая телерадиовещательная компания Эн-Би-Си (NBC) предложила Федеральной комиссии по коммуникациям (Federal Communications Commission, FCC) обязать интернет-провайдеров фильтровать все пакеты данных на наличие защищенных авторскими правами материалов (то есть принудить провайдеров проверять проходящие пакеты и задерживать те, в которых, предположительно, находятся нелегально копируемые данные). В 2002 году Конгресс согласился временно отложить реализацию запрета на *любое* коммуникационное устройство, которое не поддерживает функцию контроля авторских прав, – билль потребовалось пересмотреть после того, как выяснилось, что первоначальный вариант автоматически запрещает использование кардиостимуляторов и слуховых аппаратов.[1]

В итоге, в настоящее время в США компания, работающая в области высоких технологий, вправе разработать новое устройство управления приводом гаражных ворот, не спрашивая одобрения производителя ворот. Также компания может изготовлять альтернативные чернильные картриджи без оглядки на мнение производителей принтеров. Однако компания не вправе создавать новые программы для работы с видеодисками формата DVD без лицензии Ассоциации по контролю за копированием DVD. Компании также безоговорочно запрещается создавать новые продукты или оказывать услуги, заключающие в себе возможность обхода систем управления цифровыми правами без разрешения владельца прав, который может отвергнуть новый продукт вследствие угрозы конкуренции.

Монопольный подход к проблеме авторских прав несет гибель инновациям, направляющим цифровую эпоху.

Таково сегодня положение регулирования сторон в войнах за интеллектуальную собственность. Люди могут обсуждать преимущества этого положения. Кто-то может сказать, что Акт о защите авторских прав в цифровую эпоху необходим. Другой может возразить, что применение большинства положений акта неэффективно в сокращении числа правонарушений, поскольку увеличивается число голосов за более жесткие меры наказания. Но независимо от преимуществ монопольный подход к проблеме авторских прав несет гибель инновациям, направляющим цифровую эпоху. Он препятствует быстрому появлению новых продуктов и услуг, которые могут взаимодействовать с существующей инфраструктурой. Неопределенность правовых рисков мешает притоку инвестиций, необходимых для вывода инноваций на рынок.

[1] Акт о поддержке гражданского широковещательного и цифрового телевидения (Consumer Broadband and Digital Television Promotion Act), внесенный на рассмотрение сенатором Фрицем Холлингсом в марте 2002 года.

В сущности, Акт о защите авторских прав в цифровую эпоху поставил уголовное правосудие на службу пустым притязаниям разработчиков систем управления цифровыми правами. Акт узаконил монопольное регулирование рынка под видом защиты авторских прав. Объявив нелегальными технологии, обходящие цифровую защиту, акт, по словам одного критика, стал инструментом «фальшивой конкуренции».[1]

Группа защиты общественных интересов Public Knowledge (*publicknowledge.org*) расположена в округе Вашингтон и фокусируется на политических достижениях в области цифровой информации. Свежую информацию по этой теме можно найти в блогах «issues» и «policy» группы.

«Коянискацци» защиты от копирования: жизнь, выведенная из равновесия

1982 год отметился выходом на экран удивительного фильма под названием «Koyaanisqatsi» (Коянискацци). Название фильма – слово из языка индейцев племени хопи, означающее «существование без гармонии». Фильм, не содержащий диалогов или голоса диктора за кадром, обрушивает на зрителей как сцены невообразимо прекрасные, так и глубоко тревожащие, сцены, сопоставляющие мир природы и мир городов. Фильм безостановочно напоминает о том, что технологии отнимают у нас возможность жить счастливой, гармоничной жизнью.[2]

В первом десятилетии XXI века мы живем в мире коянискацци в области авторских прав. Почти каждый залп в войнах за интеллектуальную собственность сопровождается введением федерального законопроекта, подачей иска, судебным решением или адвокатской апелляцией, осознанием необходимости соблюдения «традиционного равновесия авторских прав» и его защитой. Истина в том, что равновесие давно нарушено, сметено цифровым нашествием, и это подобно разрушению основы для любого гражданского соглашения по управлению информацией. Равновесие разрушено во имя благих намерений.

---

[1] Тимоти Б. Ли (Timothy B. Lee) «Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act» (Конкуренция обмана: негативные последствия Акта о защите авторских прав в цифровую эпоху), Институт Катона, аналитический доклад № 564, 21 марта 2006 года, *www.cato.org/pub_display.php?pub id=6025*.

[2] См. сайт *www.koyaanasqatsi.org*. Какая ирония в том, что фильм, заслуживший у некоторых звание величайшего произведения киноискусства, был недоступен зрителям большую часть 1990-х из-за спора об авторских правах!

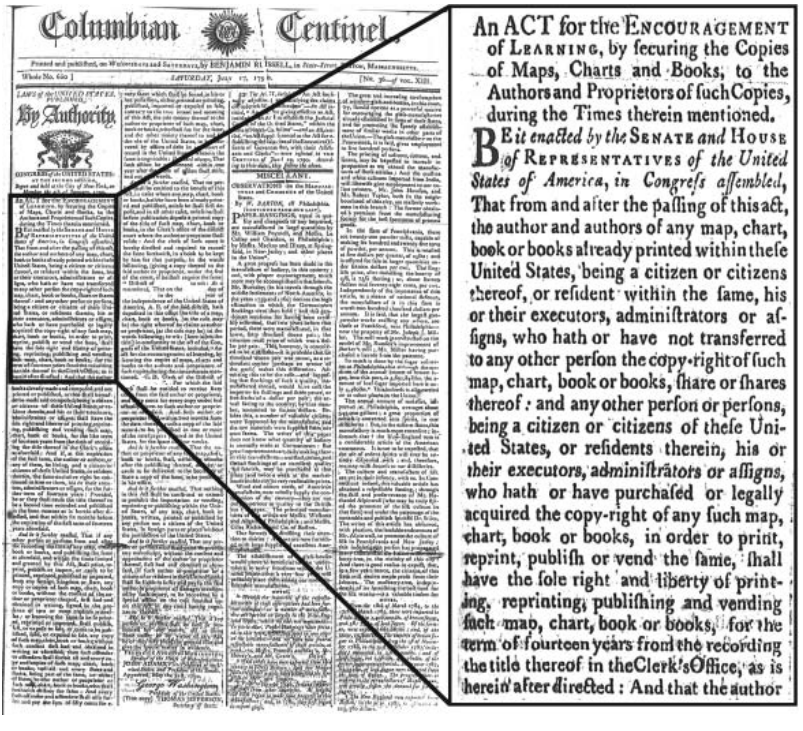
Авторское право (по крайней мере, в США) представляет собой сделку между автором и обществом при посредничестве правительства. Автор получает ограниченный монопольный контроль над произведением на ограниченный срок, обеспечивающий возможность получения коммерческой выгоды. Общество получает выгоды от использования произведения, а также неограниченную возможность распоряжаться произведением после истечения срока. Условия сделки менялись со временем, обычно в сторону усиления монополии. В первом американском законе о защите авторских прав, принятом в 1790 году, срок составлял не более 28 лет. В настоящее время срок длится 70 лет после смерти автора. Но сделка все еще остается сделкой.

Цифровая интеллектуальная собственность

Книга Джессики Литман (Jessica Litman) «Digital Copyright» (Цифровое авторское право) рассматривает эволюцию законодательства об авторском праве как серию переговоров и компромиссов. Проект «Citizen Media Law» (*www.citmedialaw.org*) предлагает полезную информацию для тех, кто публикует произведения в Интернете, – не только об авторском праве, но и о смежных областях законодательства.

Это чрезмерно сложная сделка, и легко понять, почему. Нынешнее право на интеллектуальную собственность прошло через две сотни лет споров, переговоров и компромиссов. Первый закон об авторском праве полностью уместился в пару газетных колонок газеты «Columbian Centinel» (рис. 6.3). Как видно из увеличенной вставки, положения закона охватывают карты, диаграммы и книги и дают исключительные права на «печать, перепечатку, публикацию или продажу». Длительность права автора сохраняется в течение 14 лет (с возможностью продления еще на 14 лет).[1] Текст закона, действующего в настоящее время, занимает более 200 страниц. Это запутанный документ, испещренный исключениями, поправками и предложениями, обладающими совершенно таинственным смыслом. Вы не можете публично исполнять музыкальное произведение, не являясь представителем сельскохозяйственной бригады на ярмарке. Вы не можете свободно копировать письменные документы, если не принадлежите к ассоциации слепых – тогда вы вправе сделать копию шрифтом Брайля (если только документ не является стандартизированным тестом). Радиостанция не может транслировать запись без лицензии издателя, но лицензия от студии звукозаписи не требуется – это в случае аналогового вещания.

[1] Изображение с микрофильма из библиотеки Гарвардского университета. Современный вариант доступен здесь: *www.copyright.gov/title17/circ92.pdf*.



Columbian Centinel

An ACT for the ENCOURAGEMENT of LEARNING, by securing the Copies of Maps, Charts and Books, to the Authors and Proprietors of such Copies, during the Times therein mentioned.

BE *it enacted by the* SENATE *and* HOUSE *of* REPRESENTATIVES *of the United States of America, in Congress assembled,* That from and after the passing of this act, the author and authors of any map, chart, book or books already printed within these United States, being a citizen or citizens thereof, or resident within the same, his or their executors, administrators or assigns, who hath or have not transferred to any other person the copy-right of such map, chart, book or books, share or shares thereof: and any other person or persons, being a citizen or citizens of these United States, or residents therein, his or their executors, administrators or assigns, who hath or have purchased or legally acquired the copy-right of any such map, chart, book or books, in order to print, reprint, publish or vend the same, shall have the sole right and liberty of printing, reprinting, publishing and vending such map, chart, book or books, for the term of fourteen years from the recording the title thereof in the Clerk's Office, as is herein after directed: And that the author

Рис. 6.3. *Первый в США закон об интеллектуальной собственности – Акт о поощрении образования (Act for the Encouragement of Learning). Полный текст закона напечатан в двух первых колонках выпуска газеты «Columbian Centinel» от 17 июля 1790 года. Внизу второй колонки – подпись Джорджа Вашингтона*

Библиотека Гарвардского университета

Для цифрового спутникового вещания необходимы обе лицензии (хотя есть несколько исключений).[1]

Этот закон явно составлен в расчете на специалистов, а не рядовых граждан. Даже юристы средней руки встречаются с затруднениями при интерпретации положений Акта. Впрочем, это не имеет особого значения, так как сделка об авторских правах никогда не затрагивала рядовых граждан. Так называемое «равновесие прав на интеллектуальную собственность» балансирует только вокруг оси интересов бизнеса. История эволюции авторских прав – это рассказ о нескольких главных игроках, сидящих вокруг стола и решающих дела, в то время как Конгресс обычно следует общему решению. Рядовые граждане не участву-

[1] Кодекс законов США, том 17, параграфы 110(6), 121(a)(2) и 114.

ют в игре, потому что не имеют физической возможности публиковаться – им нечего предложить в качестве ставки.

Опоздавшая ставка

Цифровая экспансия изменила расклад, предоставив каждому возможность копировать и распространять информацию по всему миру. Издателем теперь может стать любой. Общество наконец-то стало участником сделки – но игра продолжается уже двести лет, и главные сделки давным-давно заключены.

Когда люди приходят с намерением «сесть за стол» и выложить свои возможности для публикации, предполагая воспользоваться всеми преимуществами цифровых технологий, то обнаруживают восхитительные, простые и естественные возможности. Однако эти возможности уже «отбалансированы» подальше от общества. Среди потерянных возможностей – копирование содержимого дисков DVD на переносной проигрыватель, создание видеоклипа на основе звукозаписи, помещение любимой музыки или мультипликации на страницу профиля в сети Facebook или добавление собственного творчества к понравившейся работе с последующим размещением для общего доступа.

Люди возмущаются, когда подобные действия объявляются воровством или пиратством. Как мудро заметил участник одной сетевой конференции, «в первом классе мне говорили, что нужно делиться, а теперь говорят, что это незаконно».

Такое разочарование легко может породить чувство морального ущерба.[1] Вот что говорит основатель Фонда электронной безопасности Джон Гилмор:

> Нет плохого в том, что мы изобрели технологию, позволяющую сократить определенный дефицит; но мы преднамеренно отбросили ее ради получения прибыли теми, кто выигрывает от создания дефицита. Современные средства позволяют дублировать любую информацию, которая только может быть компактно размещена на цифровом носителе... Мы должны радоваться тому, что совместными усилиями создаем земной рай! Вместо этого подлые душонки, обеспечивающие свое существование за счет поддержания вечного дефицита, шныряют вокруг, убеждая сообщников прибрать к рукам наши дешевые технологии копирования, чтобы делать копии стало невозможно, – по крайней мере, для тех товаров, которые они нам продают. Это худший сорт экономического протекционизма – доводить до нищеты собственное общество ради извлечения прибыли из неэффективной местной индустрии.

---

[1] Джон Гилмор (John Gilmore) «What's Wrong with Copy Protection» (Что случилось с защитой от копирования?), 16 февраля 2001 года, *www.toad.com/gnu/whatswrong.html*.

Можно ли копировать музыкальные компакт-диски на свой компьютер?

Разумеется, это *возможно* сделать: специально для этой цели есть десятки программ, и миллионы людей делают это регулярно. Но правовые основания копирования компакт-дисков туманны и вводят в замешательство – яркий пример несоответствия законодательства и общественного знания.

Давая показания на судебном заседании по обвинению матери-одиночки Джейми Томас (см. выше в этой главе) в 2007 году, ведущий представитель обвинения со стороны корпорации Sony BMG Дженнифер Пэризер предположила, что копирование даже собственного легально купленного компакт-диска, даже только для личного использования, является противозаконным, заметив, что копирование купленной музыки – это всего лишь «„воровство еще одной копии“ в вежливой форме». На сайте Американской ассоциации звукозаписывающих компаний специально оговорено, что копирование музыки «обычно не вызывает вопросов», если копия делается для личных целей, но предупреждается, что передача копии или разрешение копировать другим является противозаконным. Напротив, опрос среди подростков Лос-Анджелеса в октябре 2006 года показал, что 63% опрошенных считают вполне законным копировать диски, приобретенные друзьями.[1]

Но копирование и распространение копий одним лицом может считаться воровством со стороны другого лица, а другая сторона в войне за интеллектуальную собственность не испытывает недостатка в собственном моральном ущербе. Киноиндустрия оценивает стоимость нелегальных копий фильмов, распространяемых через Интернет, в сумму, превышающую 7 млрд долларов. Председатель Американской ассоциации кинокомпаний заявляет:

---

[1] Показания Дж. Пэризер цитируются в статье Эрика Бэнджмана (Eric Bangeman) «Sony BMG's chief anti-piracy lawyer: 'Copying' music you own is 'stealing'» (Ведущий юрист по вопросам пиратства Sony BMG: «Копирование приобретенной вами музыки есть воровство»), *Ars technica* от 2 октября 2007 года, *http://arstechnica.com/news.ars*. Когда был задан вопрос об этом, председатель Ассоциации звукозаписывающих компаний Кэри Шерман заявил, что Дж. Пэризер «оговорилась» и неверно поняла вопрос (*Talk of the Nation* от 3 января 2008 года). Политика Ассоциации по отношению к копированию компакт-дисков здесь: *http://www.riaa.com/physicalpiracy.php*. См. также Чарльз Дьюхигг (Charles Duhigg) «Is Copying a Crime? Well...» (Копирование – это преступление? Хм...), *Times* (Лос-Анджелес) от 9 августа 2006 года, *www.latimes.com*.

> Мы не приветствуем... прикрытие воровства под маской технологии. Никакой бизнес, в том числе кинобизнес, не сможет держать свои двери открытыми, платить сотрудникам и удовлетворять потребности покупателей, если пираты и воры могут пренебрегать фундаментальным правом этой страны для частных лиц владеть их творческими произведениями и получать выгоду от произведений и права владения.[1]

Это никакое не «равновесие». Это отвратительный взаимный обстрел протестами и обвинениями, путь ужесточения наказаний и монопольного регулирования во имя права на интеллектуальную собственность. Побочный эффект – новшества остаются заложниками войны.

Движение к перемирию

Чтобы сойти с этого пути, необходимо освободиться от устаревших идей и взглядов. Трудно, на первый взгляд, но для оптимизма есть основания. В течение 2007 года медиаиндустрия сделала серьезную попытку отойти от управления цифровыми правами. Помимо ограничений на технологии, системы управления правами создают неудобства как для потребителей, так и для издателей. Понимание связанных с этим проблем растет не только среди групп, защищающих интересы потребителей, но и внутри индустрии.

Одним из первых заметных шагов в данном направлении стало объявление генерального директора корпорации Apple Стива Джобса, опубликованное в форме открытого письма к директорам предприятий медиаиндустрии (февраль 2007 года). Письмо содержало просьбу ослабить лицензионные ограничения, что понадобилось корпорации Apple для реализации системы управления правами на музыкальном сервисе iTunes. С точки зрения Стива Джобса, мир интернет-магазинов, продающих музыку, свободную от цифровой защиты и способную воспроизводиться на любом проигрывателе, будет «действительно наилучшей альтернативой для потребителей, и корпорация Apple всеми силами это поддержит».[2]

Медиаиндустрия отреагировала довольно вяло, но другие участники активно поддержали инициативу. В марте один из крупнейших в Европе музыкальных интернет-магазинов Musicload выступил против систем управления цифровыми правами, сообщив, что 75% обращений потребителей в службу поддержки было вызвано проблемами с цифровой защитой. Представители сервиса Musicload заявили, что

---

[1] Новостной выпуск «Lights... camera... busted!» (Свет! Камера!.. Взяли!) Ассоциации киностудий от 21 июня 2007 года, *www.mpaa.org/PressReleases.asp*. Цитируются слова председателя ассоциации Дэна Гликмана (Dan Glickman), комментирующего решение суда по делу пиринговой сети Grokster 25 января 2005 года, *www.riaa.com/newsitem.php/news_room.php*.

[2] Стив Джобс (Steve Jobs) «Thoughts on Music» (Размышления о музыке), 6 февраля 2007 года, *http://www.apple.com/hotnews/thoughtsonmusic/*.

системы управления правами создают трудности использования покупки для потребителей и препятствуют развитию массового рынка легального скачивания произведений. В ноябре Британская ассоциация поставщиков средств развлечения (British Entertainment Retailers Association) также выступила против систем управления цифровыми правами. Председатель ассоциации заявил, что механизмы защиты от копирования «препятствуют развитию и направлены против интересов потребителей».[1]

К началу лета 2007 года сервисы Apple iTunes и (независимо) Universal Music Group начали выпуск свободно копируемых музыкальных файлов.[2] Файлы, скачанные с сервиса iTunes, содержали информацию («водяной знак»), идентифицирующую оригинального покупателя. Таким образом, если в Интернете появится множество нелегальных копий, законного покупателя можно выследить и взять на учет.

Применение цифрового «водяного знака»

Применение цифрового «водяного знака», в отличие от ограничений на копирование и контроля доступа, – пример общего подхода к регулированию путем не *запрета*, а *учета*. Подход не препятствует нарушениям права, но позволяет распознавать их и принимать соответствующие меры. Тот же подход применяется в законе о праве на неприкосновенность частной жизни (см. главу 2), закрепляющем не ограничение доступа к персональной информации, а допустимость ее использования.[3]

---

1 Эндрю Эджклифф-Джонсон (Andrew Edgecliffe-Johnson) «Anti-piracy moves 'hurt sales'» (Антипиратские меры «вредят продажам»), *Financial Times* от 20 ноября 2007 года, *www.ft.com*.

2 «Apple Launches iTunes Plus: Higher Quality DRM-Free Tracks Now Available on the iTunes Store Worldwide» (Apple запускает iTunes Plus: записи высокого качества и без цифровой защиты теперь общедоступны на iTunes Store), 30 мая 2007 года, *www.apple.com/pr/library/2007/05/30itunesplus.html*. Также см. Кен Фишер (Ken Fisher) «Universal to track DRM-free music online via watermarking» (Universal отслеживает в сети музыку без DRM при помощи цифровых водяных знаков), 15 августа 2007 года, *arstechnica.com/news.ars/post/20070815-universal-to-track-drm-free-music-online-via-watermarking.html*.

3 Д. Вайтцнер, Х. Абельсон, Т. Бернерс-Ли, Дж. Фейгенбаум, Дж. Хендлер, Г. Зюссман (D. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, and G. Sussman) «Information Accountability» (Возможность учета информации), *MIT CSAIL Technical Report*, MIT-CSAIL-TR-2007-034, 13 июня 2007 года, *hdl.handle.net/1721.1/37600*.

Несколько месяцев спустя даже такой уровень ограничений начал сходить на нет. К началу 2008 года четыре главных медиагиганта – Universal, EMI, Warner и Sony/BMG – стали продавать на сайте Amazon музыкальные файлы, не содержащие цифровых отметок о покупателе.[1]

Эта заметная смена ориентиров произошла всего за год. Когда Стив Джобс сделал свое заявление, генеральный директор компании Warner Music Эдгар Бронфман решительно отверг идею, считая ее «абсолютно нелогичной и не заслуживающей внимания».[2] К концу года компания Warner заявила, что будет продавать на сайте Amazon цифровую музыку, не защищенную системой управления правами.[3] Попутное обращение Бронфмана к служащим гласило:

> Убрав барьеры, препятствующие продаже и получению удовольствия от скачивания музыкальных файлов, мы закончим изнурительные для нас дебаты и позволим себе переориентироваться на возможности и продукты, которые принесут выгоды не только компании, но и нашим исполнителям и покупателям.

Растущее понимание того, что подход, основанный на системах управления цифровыми правами (DRM), не оправдал себя, дает начало экспериментированию с новыми моделями распространения музыкальных произведений в Интернете.

Компания Universal провела переговоры с Sony и другими медиагигантами о создании сервиса подписки на музыку, когда пользователь за фиксированную абонентскую плату получает доступ к неограниченному количеству файлов. Другое предложение привязывает сервис к новым устройствам, в стоимость которых будет включена стоимость музыкальных произведений.[4]

Еще одно похожее решение предлагает распространение музыки посредством лицензии на мобильную связь или услуги интернет-провайдера. Появляются новые компании, предлагающие эту услугу при проектировании и формировании вычислительных сетей учебных заве-

---

1 Элиот ван Бускирк (Eliot Van Buskirk) «Some of Amazon's MP3 Tracks Contain Watermarks» (Некоторые файлы звукозаписей в формате MP3 с Amazon содержат водяные знаки), блог Wired, 25 сентября 2007 года, *blog.wired.com/music/2007/09/some-of-amazons.html*.

2 Грег Кайзер (Gregg Keizer) «Warner Chief Calls Jobs' DRM Fight 'Without Logic'» (Глава Warner называет борьбу Джобса с DRM «нелогичной»), *Computerworld* от 10 февраля 2007 года.

3 Джессика Минтц (Jessica Mintz) «Warner offers DRM-free music on Amazon» (Warner предлагает музыку без DRM на Amazon), *Associated Press* от 28 декабря 2007 года.

4 «Universal Music Takes on iTunes» (Universal Music берется за iTunes), *Business Week News* от 22 октября 2007 года, *www.businessweek.com/magazine/content/07_43/b4055048.htm?chan=rss_topStories_ssi_5*.

дений.[1] Другой вариант – *сеть неограниченного доступа* к цифровым произведениям. Такие сети могли бы предоставлять доступ к аудио- или видеозаписям, распространяемым в Интернете, без каких-либо ограничений. Пользователи смогут скачивать, копировать, делиться с другими, записывать произведения на переносные устройства до тех пор, пока произведения не распространяются за пределами Сети.[2]

Дополнительные подходы поощряют распространение музыкальных и иных творческих произведений способом, обогащающим общую культуру, путем предоставления авторам возможности распространять собственные произведения и вносить свой вклад в произведения других авторов. Одна из организаций, предоставляющих технические и правовые инструменты для реализации такого подхода, называется Creative Commons. Организация распространяет семейство лицензий, которые авторы могут использовать для публикации своих работ в Интернете (часть лицензий допускает открытое распространение работ). Лицензии реализуются как в форме правовых документов, так и в форме программного кода, который может применяться при создании новых программ. Если в Интернете появляется работа с подходящей лицензией семейства Creative Commons, то поисковые системы при поиске материалов, соответствующих определенным условиям лицензирования, могут вернуть ссылку на эту работу. Стимулирование открытой публикации работ в Интернете – это шаг навстречу *общему использованию ресурсов*; это система, которая снижает необходимость в подробно расписанных лицензионных ограничениях (в главе 8 можно узнать больше о том, что подразумевается под словами «общее использование»).

Применение приведенных и других подходов со временем покажет, какие модели распространения музыки, не использующие системы управления правами, экономически выгодны. Успех применения сможет показать киноиндустрии и другим издателям, как сойти с пути монополизации.[3] Прежний путь – это тупик, который больше тормозит нов-

---

[1] Один из примеров – Ruckus Network (*www.ruckusnetwork.com*), компания, распространяющая потоковое аудио и видео в студенческих городках. Недостаток такой модели в том, что она использует защиту DRM: файлы можно воспроизводить, но нельзя записывать на компакт-диски.

[2] Например, компания с участниками из Гарвардской школы права Noank Media; планируется сотрудничество с несколькими китайскими университетами.

[3] Пример: Брюс Леман (Bruce Lehman), помощник секретаря министра торговли в администрации президента Клинтона, главный разработчик проекта Акта о защите авторских прав в цифровую эпоху, во время обсуждения в университете Макгилла 25 марта 2007 года признал, что «наша администрация при Клинтоне работала не очень хорошо» и что «наши попытки... контроля интеллектуальной собственности не были успешными». Также он критиковал медиаиндустрию за медленное движение навстречу требованиям сетевого рынка. Видеозапись выступления: *video.google.com/videoplay?docid=4162208056624446466*.

шества, чем препятствует правонарушениям, подход, который даже некоторые из его создателей признают провалом.

Но тем не менее даже тогда важнейшие проблемы, порожденные Актом о защите авторских прав в цифровую эпоху, не будут решены, поскольку закрепленные в законе правила нелегко изменить. Если медиаиндустрия переходит на более эффективные модели ведения бизнеса и битва за системы управления правами утихает, то положения акта все еще остаются антипользовательскими и антиконкурентными участками цифрового ландшафта. До тех пор пока положения акта не будут отменены, они так и останутся реликтовыми трофеями с полей битв той войны, которая была улажена мирными средствами – неразорвавшимися снарядами, которые бизнес все еще может использовать обратно изначальным целям создания акта.

Лицензии Creative Commons

Создавая работы для публикации в Интернете, с помощью генератора Creative Commons (*creativecommons.org*) вы можете получить лицензию, подходящую лично вам. Имея лицензию, вы можете сохранить важные для вас права, одновременно позволяя использование другими людьми несущественных прав.

Пределы собственности

Пятнадцать лет цифровая музыка и фильмы находились на линии фронта войн за интеллектуальную собственность. Возможно, приостановить эти сражения помогут грядущие инновации и эксперименты. Безграничный потенциал Интернета для добрых – и выгодных – дел не должен быть принесен в жертву злоупотреблениям. Если вам не нравится то, что другие делают с Интернетом, это не значит, что Интернет станет вашим врагом – до тех пор, пока вы его не сделаете таковым.

Напряжение вокруг интеллектуальной собственности очень высоко. Интерес к новым подходам, таким как учет пользователей и сообщества, предполагает высокий уровень недовольства метафорами собственности и воровства, применяемыми к текстам и музыке. Равновесие прав на интеллектуальную собственность, нарушенное с приходом цифровой эпохи, является чем-то большим, нежели традиционное противостояние автора и потребителей. Это равновесие между личностью и обществом, на котором основаны наши понятия о собственности. Учет пользователей или сообщества – это попытки противостоять росту ограничений прав собственности, установленных во имя соблюдения цифрового авторского права.

Обозначая кино, музыку и книги словом «собственность», мы оперируем примитивными понятиями свободы и независимости: «Это твой участок земли, а это мой участок земли». Но цифровые технологии уничтожили эти понятия. «Мой участок» может отличаться от «твоего участка», но когда оба участка распылены на облака битовой пыли, эти облака сливаются. А границы собственности, разделявшие участки, пропадают в тумане сетевых пакетов данных.

Учимся летать в цифровых облаках

В 2004 году корпорация Google запустила новый проект (см. главу 4) индексирования книжного фонда нескольких крупнейших библиотек для поисковой системы Google. Цель проекта состояла в том, чтобы при обращении к поисковой системе можно было найти по ключевым словам подходящую книгу вместе с отрывком текста. Как сообщалось, проект был нацелен на «создание всеобъемлющего виртуального каталога для поиска любых книг на любых языках», и это не должно было вызывать больше споров, чем обычный библиотечный каталог.

Ассоциация американских издателей и Гильдия авторов (Authors' Guild) обратили внимание на новый проект и подали иск против корпорации о нарушении авторских прав. По словам председателя ассоциации Патриции Шредер, «корпорация Google собирается заработать миллионы долларов на эксплуатации талантов и собственности авторов и издателей». Президент гильдии приравнял включение книги в проект к ее краже. Сотрудники корпорации Google собирались сканировать книги и делать копии для индексирования[1]; таким образом, поводом для судебного рассмотрения стал вопрос о легальности применения данных технических средств по отношению к авторским правам.

Библиотечный проект определенно выгоден для корпорации Google, так как повышает конкурентоспособность ее поисковой системы, и корпорация определенно сканирует книги без разрешения правообладателей. Присваивает ли корпорация чужую собственность, извлекая прибыль без отчислений авторам или хотя бы их разрешения? Следует ли просить

[1] Описание проекта Google books: *books.google.com/googlebooks/library.html*. Иски описаны в статье Элинор Миллс (Elinor Mills) «Authors Guild Sues Google over library project» (Гильдия авторов судится с Google из-за библиотечного проекта), CNET News.com от 20 сентября 2005 года, *news.com.com/2100-1030 3-5875384.html*; статья Элори Гилберта (Alorie Gilbert) «Publishers sue Google over book search project» (Издатели судятся с Google из-за проекта сервиса поиска по книгам), 19 октября 2005 года, *news.com.com/Publishers+sue+Google+over+book+search+project/2100-1030_3-5902115.html*. Комментарии президента Гильдии авторов Ника Тэйора есть в дебатах о статье, появившейся в публичной библиотеке Нью-Йорка 17 ноября 2005 года, стенограмма здесь: *www.nypl.org/research/calendar/imagesprog/google111705.pdf*.

разрешения? Если вы написали книгу и это – «собственность», которой вы «владеете», как далеко простираются ваши права?

Как общество, мы уже сталкивались с этим вопросом. Если через ваш участок течет ручей, владеете ли вы его водой? Где пределы ваших прав? Можете ли вы выкачать воду и продать ее – даже если это приведет к нехватке воды ниже по течению? Это были основные поводы для разбирательств на Западе США в XIX веке, что привело к созданию сложной системы законов об ограничении права собственности землевладельцев на протекающие через их участки водные потоки.[1]

Культура свободы

Книга Лоуренса Лессига (Lawrence Lessig) «Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity» (Свободная культура: как медиагиганты с помощью технологии и закона устраняют необходимость культуры и контролируют творческий потенциал) увлекательно прослеживает историю того, как чрезмерные лицензионные ограничения угрожают будущему здоровой и полноценной общественной культуры.

Представьте, что над вашей землей летит самолет. Это нарушение границ частных владений? Самолет летит очень низко. На какую высоту простирается ваше право собственности? С древнейших времен права собственности простирались вверх неограниченно.[2] Возможно, авиалиниям необходимо запрашивать разрешения на полет у каждого землевладельца, над чьим участком пролегает маршрут полета. Пред-

[1] В США частности этого права «прибрежной полосы» различаются от штата к штату. Первое дело такого рода рассматривалось в 1891 году: «Стриклер против Colorado Springs», 16 Colo. 61, 70, 26 P. 313, 316 (1891). За аналогию информации и воды спасибо Дэвиду Вайтцнеру.

[2] Для обсуждения с точки зрения живших в 1920-е см. Хирам Л. Джоум, (Hiram L. Jome) «Property in the Air as Affected by the Airplane and the Radio» (Собственность в воздухе и ущерб от аэропланов и радио), «The Journal of Land & Public Utility Economics», т. 4, № 3 (август 1928), с. 257–272. «Формула римского общего права начала XVI в. <звучит так>: «Cuius est solum, eius est usque ad caelum» («Кто владеет землей, владеет ей до самого неба»). Автор книги приводит пример владельца «Птичьей фермы „Кудахчущий уголок“», который обратился к почтовому министру с заявлением о том, что низко пролетающие почтовые аэропланы пугают кур и снижают яйценоскость. Акт о воздушной торговле 1926 года (Air Commerce Act) национализировал полетное воздушное пространство. Интересно сравнить этот факт с национализацией частотного диапазона (см. главу 8).

ставьте, что задаетесь этим вопросом на заре эры воздухоплавания. Нужно ли заставлять авиалинии приобретать разрешение на полеты ради соблюдения прав собственности? Это могло показаться разумным во времена, когда самолеты могли подняться максимум на 300 метров. Но тогда какой смысл был бы в развитии авиации? Смогли бы мы увидеть трансконтинентальные полеты, или этот путь затерялся бы в чаще прав и разрешений? Конгресс расчистил заросли, приняв закон о национализации полетного воздушного пространства в 1926 году.[1]

Интеллектуальная собственность и поисковые сервисы

Если вы считаете, что библиотечный проект корпорации Google нарушает авторские права, то можете предположить, что и сам по себе сервис поиска их нарушает, так как копирует и индексирует веб-сайты, выдавая ссылки на копии. Этот факт послужил поводом к нескольким судебным разбирательствам, в большинстве случаев решенных в пользу поисковых компаний. В деле «Field против Google» (январь 2006 года) окружной суд штата Невада признал кэширование и индексирование веб-страниц сервисом Google не противоречащим закону. На решение суда повлиял в том числе факт, что кэшированные страницы хранятся только временно. В деле «Perfect 10 против Google» (май 2007 года) апелляционный суд отказал в иске журналу для совершеннолетней аудитории о запрете сервису Google возвращать ссылки на сайт журнала и помещать уменьшенные копии изображений с сайта.

Рассуждая подобным образом, следует ли требовать от корпорации Google получать разрешение от каждого владельца прав на книгу перед индексированием содержимого книги? Это кажется вполне разумным – и другие разрабатываемые проекты по индексированию книг действительно запрашивают разрешения. Но возможно, поиск по текстам книг – это цифровой эквивалент малой авиации. Можем ли мы

[1] Параллель между воздушными и информационными правами проведена Ларри Лессигом (Larry Lessig) в книге «Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity», Penguin, 2004 год; а до него об этом упоминал Кейт Аоки (Keith Aoki) в статье «(Intellectual) Property and Sovereignty: Notes toward a Cultural Geography of Authorship» (Интеллектуальная собственность и владение: заметки о культурной географии авторства), *Stanford Law Review*, т. 48, № 5 (May 1996), с. 1293–1355. В 1976 году Эквадор, Колумбия, Бразилия, Конго, Заир, Уганда, Кения и Индонезия подписали Боготскую декларацию, которая объявляла право национального суверенитета экваториальных стран на отрезки геостационарных орбит над территориями участников.

представить себе будущее, когда книги, музыка, изображения и фильмы автоматически копируются, делятся на фрагменты, комбинируются снова и снова, заносятся в объемные системы автоматической обработки, становятся доступными из обязательного для каждого компьютера или мобильного телефона программного обеспечения и происходят тысячи других вещей, для которых пока нет даже названия?

Каким должно быть истинное равновесие? Как далеко в расширяющемся информационном пространстве должны простираться права собственности? Что вообще должно означать понятие собственности, когда речь заходит о битах? Мы не знаем ответов и думаем, что найти их будет нелегко. Но так или иначе, мы должны научиться летать.

Цифровой взрыв разбрасывает информацию в разные стороны, ломая установленные границы собственности. Технологии сделали неэффективным те правила, которые должны были бы направлять и удерживать биты в полете, – авторские права. Чтобы справиться с проблемами, созданными технологиями, были найдены технологические же решения. Эти решения создали *де-факто* права владения битами, упустив из виду общественные интересы, соблюдение которых должно было уравновесить права на интеллектуальную собственность.

Границы собственности – это не только преграды, разрушенные нашествием, а право на интеллектуальную собственность – не только арена, на которой брошен вызов информационному регулированию. Биты могут перелетать через государственные границы. Биты влетают в частные дома и общественные места, принося нежелательную или даже вредоносную информацию – информацию, исторически ограничиваемую даже не авторским правом, а законами против клеветы или порнографии. Биты летают повсюду – это загадка, решением которой мы теперь и займемся.

Глава 7 | О чем нельзя говорить в Интернете

Охрана границ свободы цифрового слова

Знаете ли вы, какие сайты посещал сегодня ваш ребенок?

Случилось то, чего больше всего боятся все родители. В июне 2006 года пропала Кэтрин Лестер, 16-летняя отличница из деревни Фэйргроув (Мичиган). Ее родители не имели ни малейшего представления о том, что произошло; девушка никогда не давала повода для беспокойства. Лестеры обратились в полицию. К работе подключились федеральные власти.

Через три дня томительной безвестности девушка нашлась, живая и здоровая – в Аммане (Иордания).

Деревня Фэйргроув слишком мала – там нет даже почты, а семья Лестеров жила в последнем доме глухой улицы. В прежние времена вселенная Кэтрин ограничивалась бы расположенной в шести милях школой, где она училась. Но в Интернете ей был доступен весь мир. Кэтрин Лестер познакомилась с Абдуллой Джимзави из Палестины, точнее из города Иерихон на западном берегу Иордана. Девушка прочла его профиль в социальной сети MySpace и отправила сообщение: «ты милый».[1] С помощью электронной почты молодые люди быстро узнали все друг о друге. Кэтрин хитростью выманила у матери свой паспорт и отправилась на Ближний Восток.[2] Когда представители американских властей встретили ее самолет в Аммане, девушка согласилась вернуться домой и извинилась перед родителями за доставленное беспокойство.

---

[1] Эрин Альберти (Erin Alberty) «A love that clicked» (Любовь по ссылкам), *Saginaw News* от 10 декабря 2006 года.

[2] Дэвид Гудман (David N. Goodman) «Michigan girl heading home from Jordan after attempted rendezvous with man she met on MySpace.com» (Девушка из Мичигана направляется домой из Иордании после попытки свидания с человеком, встреченным в MySpace.com), *Minneapolis Star-Tribune* от 9 июня 2006 года.

Месяц спустя сенатор от штата Иллинойс Джуди Бигерт выступила в Палате представителей с поддержкой нового Акта об удалении сетевых хищников (Deleting Online Predators Act, DOPA). «*MySpace.com* и другие социальные сети стали новыми угодьями охотников за детьми», – заявила сенатор Бигерт, отметив, что «все ужаснулись» случившимся с Кэтрин Лестер. «Как минимум, необходимо дать родителям хоть какую-то уверенность в том, что их дети не попадутся в ловушку при использовании Интернета в школах и библиотеках, которые финансируются государством». Законопроект предполагал потребовать от названных учреждений, чтобы они запрещали детям использовать компьютеры для общения в чатах (сетевых «комнатах для бесед») и социальных сетях без присмотра взрослых.

Один за другим выходили сенаторы на трибуну, пытаясь привлечь внимание к важности защиты детей от «сетевых хищников», но законопроект поддержали не все. Текст является «сложным и противоречивым», заметил один из сенаторов. Оригинальный проект включал не только сеть MySpace, но и магазин Amazon и источник знаний – Википедию. Эти сайты в чем-то похожи на сеть MySpace – там пользователи могут создавать учетные записи и неограниченно обмениваться информацией через Всемирную паутину. Хотя законопроект мог обеспечить защиту детей от мест, где можно было бы встретить друзей (или «хищников»), он также закрыл бы доступ к сетевым энциклопедиям и интернет-магазинам, которые сильно зависят от участия пользователей.

Вместо того чтобы потратить некоторое время на более точное определение опасных сетевых ресурсов, инициаторы проекта наспех переписали его так, чтобы определения в тексте проекта вообще не оказалось. Решение о том, какой тип сетевого ресурса подпадает под действие акта, оставили Федеральной комиссии по коммуникациям. Кое-кто ворчал, что протолкнуть явно сырой проект по защите детей инициаторов побудили надвигающиеся промежуточные выборы; проект мог оказаться неэффективным и даже противоречащим конституции.

Есть множество мест, где дети могут воспользоваться компьютерами; ограничение доступа только в школах и библиотеках едва ли отвадит подростков от сети MySpace. Только самые авторитарные родители могут честно ответить на вопрос, который газета «USA Today» задала в статье, посвященной «киберхищникам»: «Сейчас 23:00. Вам известно, какие сайты ваш ребенок просматривает сегодня вечером?»[1]

Статистика непредусмотренного развития событий действительно ужасает. Департамент юстиции произвел тысячи арестов за «заманивание в киберпространстве» – почти всегда люди среднего возраста при помощи социальных сетей завлекали подростков на собрания, что порой за-

[1] Джулиан Шер (Julian Sher) «The not-so-long arm of the law» (Не-особо-длинные руки закона), *USA Today* от 11 мая 2007 года.

канчивалсь плачевно. Ответом Американской ассоциации библиотек на Акт об удалении сетевых хищников стало заявление, что именно разъяснение, а не запрет является «ключом к безопасному использованию Интернета». Учащиеся должны учиться совместно работать в Сети, поскольку ее использование со всеми возможностями для общения является базовым средством нового, проникнутого глобальными связями мира бизнеса, обучения, а также гражданского и политического участия в жизни общества.

И, возможно, проникнутого глобальными связями мира истинной любви. История Кэтрин Лестер приобрела неожиданный поворот. С того времени как Кэтрин была найдена в Иордании, девушка настойчиво повторяла, что собиралась выйти замуж за Джимзави. Сам Джимзави, которому в то время было двадцать, говорил, что влюблен в Кэтрин Лестер, и это подтверждала мать Джимзави. Юноша просил Кэтрин рассказать ее родителям правду, но девушка отказалась. После возвращения Кэтрин Лестер власти поставили ее на учет как сбежавшую из дома и отобрали паспорт. Но 12 сентября 2007 года, когда Кэтрин исполнилось восемнадцать и она стала совершеннолетней, девушка снова полетела на Ближний Восток, чтобы наконец-то встретиться со своим возлюбленным.[1] История закончилась несколько недель спустя обменом обвинениями и возражениями, включая намеки на то, что внимание Кэтрин Лестер привлек кто-то еще. Не было никаких высокотехнологичных поводов к разрыву – кроме сюжета в телешоу Доктора Фила.[2]

Революция в цифровых коммуникациях разрушила вековые представления о человеческих взаимоотношениях – как люди встречаются, изучают друг друга, решают вопрос о взаимном доверии. В то же время революция в цифровой информации в форме веб-страниц и скачиваемых фотографий дала миллионам пользователей материалы, которые еще несколько лет назад невозможно было найти без серьезных усилий и затрат.

Политические диссиденты в китайских интернет-кафе могут (если осмелятся) читать продемократические блоги. Люди по всему миру, стыдящиеся своих болезней, страдающие от своей половой принадлежности или стремящиеся общаться с меньшинством, придерживающимся общих взглядов, могут найти факты, мнения, советы и компанию. Дети, слишком маленькие, чтобы ходить по улицам без родителей, могут смотреть жуткую порнографию прямо на семейных компьютерах. Может ли общество контролировать, что их члены видят и с кем они разговаривают?

---

1 *abclocal.go.com/wjrt/story?section=local&id=5653762*

2 «MySpace Teen breaks up on ‘Dr. Phil’» (Подростки в MySpace в восторге от «Доктора Фила»), *WNEM.com* от 27 ноября 2007 года, *www.wnem.com/news/14702796/detail.html*.

Как назвать то, не знаю что?

Акт об удалении сетевых хищников, не получивший силу закона, – одна из недавних битв в долгой войне конфликтующих течений. С одной стороны, общество заинтересовано в том, чтобы держать нежелательную информацию подальше от детей. С другой стороны, общество в целом заинтересовано в увеличении открытости связей. Конституция США защищает свободу слова. Снова и снова общество борется за поиск метафоры для электронных коммуникаций, которая отражала бы их как средства информации из прошлого, одновременно описывая их нынешнее состояние. Законы и нормы построены на традициях; только понимая аналогии, можно расширить принципы свободы слова из прошлого на новые условия настоящего – или сознательно переступить через них.

Какие законы следует применять? Интернет не похож ни на что другое. Если сравнить создание веб-сайта с изданием книги, то, возможно, следует применять законы о публикации книг. Это был принцип Интернета типа Web 1.0 – публикация для «издателей» и просмотр для пользователей. В динамичной и доступной для совместной работы инфраструктуре Web 2.0 сайты, подобные MySpace, непрерывно изменяются в соответствии с действиями пользователей. Если вы отправляете сообщение электронной почты или делаете запись в блоге, это можно сравнить с телефонным звонком или, например, вызовом конференц-связи; пожалуй, следует начать с законов, регулирующих телефонные разговоры. Идеальной метафоры пока нет. Возможно, более адекватной аналогией будет телевидение, так как просмотр веб-страниц подобен переключению каналов – исключая тот факт, что движение идет в обе стороны, а число «каналов» не ограничено.

Ниже уровня программного обеспечения Всемирной паутины и электронной почты находится собственно инфраструктура Интернета. Программное обеспечение Интернета отвечает лишь за доставку битовых пакетов, не обращая внимания на то, чем они являются, – частями книг, фильмов, текстовых сообщений или голосовыми данными, – а также независимо от того, направляются ли биты веб-броузеру, телефону или кинопроектору.

Джон Перри Барлоу, бывший текстовик группы Grateful Dead и сооснователь Фонда электронной безопасности, использовал поразительную метафору для описания Интернета в том виде, в каком он ворвался в сознание обывателей в середине 1990-х. По словам Джона Барлоу, мировое управление потоками информации долгое время контролировало перевозку вина в бутылках. В «плотском пространстве» – физическом мире – применяются различные правила для книг, почты, радиопередач и телефонных разговоров – различные типы бутылок. Теперь вино само по себе свободно течет по сети, представляя собой ничто иное, как биты, освобожденные от тары. Что-то вкладывается на

входе, и на выходе окажется тем же самым. Но в промежутке все это одна и та же субстанция – просто биты. Каковы же правила киберпространства – правила для самих битов?[1]

Когда информация передается между двумя узлами (неважно – письмо, речь, изображения или фильм), всегда есть источник и приемник. Еще может быть несколько промежуточных узлов. В аудитории слушатели воспринимают лектора непосредственно, хотя владелец помещения тоже важен для создания возможности коммуникации. У книг есть авторы и читатели, посредники между ними – издатели и продавцы книг. Естественно было бы назначить аналогичные роли участникам интернет-коммуникации и когда происходит то, чего не должно быть, возложить ответственность на одну или несколько сторон. Например, когда Пит Солис познакомился с четырнадцатилетней девушкой («Джейн Доу») по ее профилю в сети MySpace и, как она утверждает, изнасиловал ее при встрече, родители девушки предъявили сети MySpace иск на 30 миллионов долларов за пособничество изнасилованию.[2]

Интернет имеет сложную структуру. Источником и приемником могут быть друзья, обменивающиеся сообщениями электронной почты, коммерческий веб-сайт и клиент, один из офисов компании, который отправляет макет рекламной брошюры, и другой ее офис, получающий макет на другом конце света. И у источника, и у приемника свои провайдеры. Провайдеры соединены маршрутизаторами с помощью оптоволоконных кабелей, спутников связи и так далее. Пакет, путешествующий по Интернету, может пройти через устройства и линии связи, принадлежащие десяткам участников.

Для удобства (и следуя стилю профессора интернет-права Джонатана Зиттрейна) назовем группу устройств, соединяющих провайдеров, «облаком». Как показано на рис. 7.1, сигнал в Интернете идет от источника к его провайдеру, затем в «облако», из «облака» к провайдеру приемника и, наконец, к приемнику (более подробно «облако» описано в главе 3).

Если правительство собирается контролировать общение в Интернете, то может атаковать несколько разных точек.[3] Можно контролировать источник или его провайдера, объявив противоправным некоторый вид общения. Но это может не сработать, если источник находится не в той же стране, где приемник. Можно попытаться контролировать приемник, запретив получение определенных видов информации. В США

---

[1] Джон Перри Барлоу (John Perry Barlow) «The economy of ideas» (Экономика идей), май 1994 года, *www.wired.com/wired/archive/2.03/economy.ideas_pr.html*.

[2] Элисон Гувер (Alison Hoover) «Keeping MySpace safe» (Сохраняя MySpace безопасной), *The Washington Times* от 28 июня 2006 года.

[3] Анализ и рисунок основаны на работе Джонатана Зиттрейна (Jonathan Zittrain) «Internet Points of Control» для получения степени бакалавра гражданского права (2003 год).

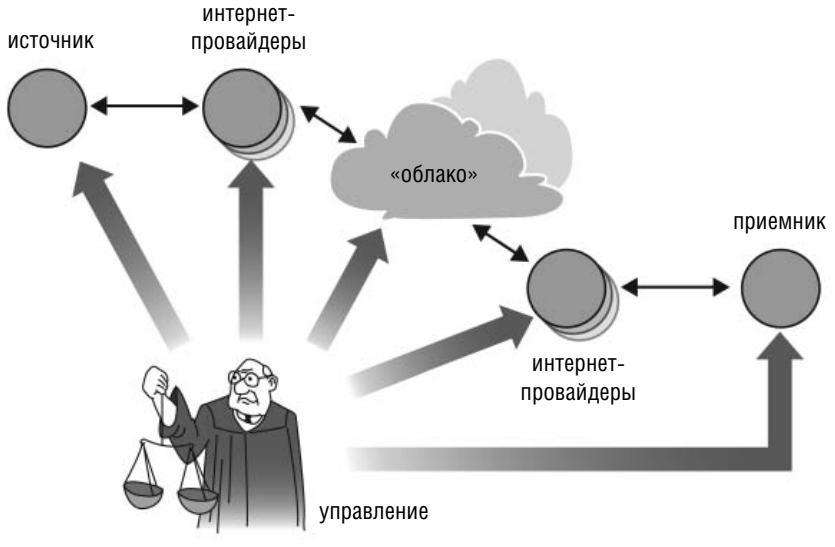


Рис. 7.1. *В каких точках управлять Интернетом?*

На основе рисунка профессора интернет-права Джонатана Зиттрейна (Гарвардский университет)

использование программного обеспечения без лицензии запрещено законом, равно как и использование иных материалов, защищенных авторским правом, с целью получения прибыли от повторного распространения.

Если в стране развито право на неприкосновенность частной жизни, то правительству нелегко узнать, что могут хранить граждане. В обществе, подобном американскому, где граждане обладают широкими правами, одиночное преследование за нелегальное хранение неэффективно. В качестве последней альтернативы государство может попытаться контролировать промежуточные звенья.

Здесь прослеживаются параллели с гражданским правом. Родители Джейн Доу судились с социальной сетью MySpace, так как это было промежуточное звено между Питом Солисом и девушкой, хотя никто из руководства сети не обвинялся в соучастии в нападении.

Законы о клевете уже давно нужно было приспособить к регулированию Интернета. В США заявление считается клеветой, если оно ложно, сообщено третьим лицам и наносит ущерб чьей-то репутации.

В реальном мире, когда кто-то клевещет на кого-то, другие слушатели могут разделять или нет ответственность за клевету. Если авторы этой книги возведут на кого-то напраслину, то этот кто-то может предъявить иск авторам, а также издателю, который мог знать, что рукопись

содержит заведомо ложные сведения. С другой стороны, водитель грузовика, отвозивший книги в магазин, пожалуй, не виноват, хотя и он вроде бы способствовал донесению лжи до читателей. На кого больше похожи электронные промежуточные звенья передачи данных – на издателей или на водителей? Был ли у родителей Джейн Доу повод обвинять сеть MySpace?

Общество изо всех сил пытается найти правильные метафоры для описания звеньев электронной коммуникации. Чтобы понять эту часть истории электронной информации, попробуем вспомнить электронные коммуникации, существовавшие до появления Интернета.

Публичная клевета

Порочащие заявления о публичных деятелях, даже ложные, не являются клеветой, если не были сделаны со злым умыслом. Эта оговорка защищает средства массовой информации от исков публичных деятелей, которые могут почувствовать себя оскорбленными теми способами, какими подает деятелей пресса. Однако это не всегда так. Самым громким из таких исков было дело «Компания „New-York Times“ против Салливана» (№ 376 U. S. 254, 1964 год), когда официальные лица штата Алабама предъявили газете иск за публикацию рекламных сообщений о гражданских правах. Эта история вместе с историей о принятии Первой поправки подробно изложена в книге Энтони Льюиса (Anthony Lewis) «Make No Law» (Обойдемся без закона). Продолжение дел, связанных с Первой поправкой, описано в книге «Freedom for the Thought That We Hate» (Свобода для мыслей, которые мы ненавидим) того же автора.

Издатель или распространитель?

Одним из ранних поставщиков компьютерных услуг, включая электронные доски объявлений и другие сообщества, в которые пользователи могли вступать за плату, была компания CompuServe. Одним из сообществ был форум Rumorville USA, поддерживающий ежедневный бюллетень с сообщениями о радиожурналистике и журналистах. Компания CompuServe не просматривала и даже не накапливала публикации форума Rumorville, получая их через посредника – компанию Don Fitzpatrick Associates (DFA). Полученные от DFA данные служба CompuServe публиковала, не просматривая. Довольно долго все было в порядке.

В 1990 году компания Cubby создала конкурирующий сервис Skuttlebut, также предоставлявший свежие сплетни о теле- и радиовещании.

На форуме Rumorville появились новые сообщения, которые называли сервис Skuttlebut «новоявленным жульничеством», утверждая, что материалы сервиса украдены с форума Rumorville. Компания Cubby подняла шум и обвинила CompuServe в клевете. CompuServe ответила, что сообщения пользователей – клевета, но что компания не издатель информации, а всего лишь распространитель – она просто передает подписчикам то, что сама получает от других. Служба CompuServe отвечает за содержимое информации не больше, чем водитель грузовика за клеветнические произведения, которые было поручено отвезти в магазин.

Какая аналогия правильна? С чем можно сравнивать компанию CompuServe – с газетой или с грузовиком, доставляющим партию газет читателям?

С грузовиком – постановил суд. Многолетняя правовая традиция освобождает распространителей от ответственности за содержимое доставляемых публикаций. Нельзя ожидать от распространителей, чтобы они прочитали все книги из грузовика. В поисках более точной аналогии судья описал сервис CompuServe, как «электронную коммерческую библиотеку». Рапространитель или библиотека, компания CompuServe не зависела от компании Don Fitzpatrick Associates и не могла нести ответственность за клеветническое содержимое поставляемой информации. Дело «Cubby против CompuServe» было безоговорочно решено в пользу компании CompuServe.[1] Компания Cubby могла проследовать до источника проблемы, но этот источник – не сервис CompuServe. Сервис был всего лишь исправно действующим промежуточным звеном. Несколько лет спустя в таком же положении оказалась социальная сеть MySpace, когда родители Джейн Доу обвинили сеть в пособничестве изнасилованию. Именно на основе решения по делу «Cubby против CompuServe» суд вынес решение о снятии ответственности с сети MySpace.

Когда закончилось рассмотрение дела «Cubby против CompuServe», поставщики компьютерных услуг вздохнули свободно. Если бы решение было иным, то электронное распространение информации стало бы рискованным делом, за которое возьмутся немногие. Компьютерные сети создали информационную инфраструктуру с беспрецедентно низкими расходами. Несколько человек, вложив совсем немного, могут помогать связаться друг с другом десяткам тысяч, даже миллионам людей. Если бы все распространяемые сведения перед их размещением на сервисе приходилось прочитывать, чтобы удостовериться, что все обличающие заявления соответствуют истине, то демократическая ценность такого сервиса свелась бы к нулю. Некоторое время царил дух свободы.

---

[1] «Cubby против CompuServe», № 90 Civ. 6571 (PKL), суд Южного округа Нью-Йорка, 29 октября 1991 года.

Ни свободы, ни безопасности

«Закон часто требует пожертвовать частью свободы ради большей безопасности. Однако иногда свобода отбирается, чтобы уменьшить нашу безопасность».[1] Так писал профессор права Калифорнийского университета в Лос-Анджелесе Евгений Волок осенью 1995 года, комментируя судебное дело, сходное с «Cubby против CompuServe», но закончившееся иначе.

В своем блоге *volokh.com* Евгений Волок регулярно комментирует события, связанные со свободой информации, и многое другое.

Компания Prodigy (подобно CompuServe) являлась поставщиком компьютерных услуг. Но в 1990-х, когда начало расти беспокойство по поводу увеличения количества материалов на сексуальные темы, компания решила позиционироваться как семейно-ориентированный сервис, взяв на себя обязательство контролировать содержимое сообщений на сетевых конференциях. В заявлении компании говорилось: «Мы не собираемся приносить извинения за то, что следуем системе ценностей, отражающей культуру миллионов американских семей, членов которых намереваемся обслуживать. Определенно, ни одна уважаемая газета не делает меньше».

Успех компании на рынке превзошел ожидания, несмотря на то что посетители ощутили меньший уровень конфиденциальности при посещении сетевых форумов по сравнению с аналогичными неконтролируемыми сервисами.

Одна из сетевых конференций сервиса Prodigy под названием «Money Talk» была посвящена финансовым услугам. В октябре 1994 года некто анонимно разместил в конференции сообщения об инвестиционной компании Stratton Oakmont. В сообщениях указывалось, что компания подозревалась в «крупном мошенничестве», ее директор был «уличен в преступлениях», а сама компания представляла собой «кучку брокеров, которые лгали, чтобы не быть уволенными».[2]

Компания Stratton Oakmont подала иск на сервис Prodigy за клевету, объясняя это тем, что сервис должен нести ответственность как издатель порочащих заявлений. На возмещение ущерба истец потребовал 200 миллионов долларов. Руководство компании Prodigy, сославшись

---

[1] Евгений Волок (Eugene Volokh) «Chilled Prodigy» (Пугающее чудо), *Reason*, август/сентябрь 1995 года.

[2] «Stratton Oakmont, Inc. и Daniel Porush против Prodigy Services», № 31063/94, верховный суд штата Нью-Йорк, округ Нассау, 24 мая 1995 года.

на решение по делу «Cubby против CompuServe», заявило, что не несет ответственности за действия посетителей форумов.

В решении, ошеломившем интернет-сообщество, суд Нью-Йорка признал компанию Prodigy виновной. Судья постановил, что компания, взявшись контролировать работу своих сервисов для поддержки добропорядочного имиджа, автоматически стала издателем со всем вытекающим объемом обязанностей и ответственности. Уравняв себя в правах с газетным изданием, компания Prodigy не могла рассматриваться как нечто меньшее. Это было так же логично, как и выбор из двух аналогий – распространитель или издатель. В реальности, однако, поставщик компьютерных услуг не является ни тем, ни другим. Проверка сообщений пользователей является весьма бледной формой редакционной работы. Невозможно проверить истинность всех сообщений.

Как бы то ни было, решение суда похоронило попытки создать «тихие гавани» в Киберпространстве. Этим решением всем администраторам конференций было дано ясное указание: даже не пытайтесь редактировать сообщения или подвергать их цензуре. Если вы это сделаете, то на основе решения по делу «Stratton Oakmont против Prodigy» будете нести ответственность за любое пропущенное умышленно вредоносное сообщение. А если вы ничего не меняете, то решение по делу «Cubby против CompuServe» автоматически освобождает вас от любой ответственности за содержание сообщений.

Такой вариант действий обеспечивает безопасность администраторов сайтов, но не всегда соответствует интересам общественности. Это в некотором роде угроза свободе слова, потому что меньшее количество добропорядочных семей пожелает читать непристойности, которые могут появиться на сайтах, позволяющих печатать все, что угодно, даже явную клевету. Одновременно снижается уровень безопасности.

Самое отвратительное место на Земле

Каждая технология в области коммуникации используется как для контроля, так и для содействия потоку идей. Всего через столетие после выхода Библии Гутенберга папа Павел IV приказал отпечатать список из 500 запрещенных авторов. Первая поправка к Конституции США защищает авторов и ораторов от правительственного принуждения: «Конгресс не должен издавать ни одного закона... ограничивающего свободу слова или печати...» Но эта защита не является абсолютной. Никто не имеет права публиковать непристойные материалы. Правительство имеет право уничтожить материалы, если докажет их непристойность, как сделало почтовое управление в 1919 году, предав огню журналы с цитатами из «Улисса» Джеймса Джойса.

В истории США было множество правовых дебатов о том, что считать непристойностью. В настоящее время суды главным образом руководствуются решением Верховного суда по делу «Миллер против штата

Калифорния»; это называют *тестом Миллера*. Чтобы определить, является ли материал непристойным, суд должен принять решение о следующем:

1. Вызывает ли в целом рассматриваемая работа у среднестатического гражданина, следующего общепринятым стандартам, похотливый интерес.
2. Изображает или описывает рассматриваемая работа явно оскорбительным образом сексуальное поведение, специально определенное соответствующим законом штата.
3. Имеет ли в целом рассматриваемая работа отрицательную литературную, художественную, политическую или научную ценность.

Что такое «общество» в Киберпространстве?

Работа признается непристойной, только если на все вопросы дан положительный ответ. Тест Миллера привязан к местности, так как нет государственных стандартов непристойности. Есть только «общественные» стандарты, которые могут сильно отличаться в разных штатах. Но в 1973 году не было компьютерных сетей. И что означает понятие «общество» (community) в Киберпространстве?

В 1992 году Всемирная паутина находилась в зачаточном состоянии, и многие американцы использовали коммутируемое подключение для доступа к централизованным электронным доскам объявлений. Некоторые из них были бесплатными и объединяли сообщества по интересам – например, любителей бейсбола или певчих птиц. В других сообществах распространялись бесплатные программы. Боб и Карлин Томас из Мильпитаса (Калифорния) создали сервис Amateur Action, который они сами называли «самым отвратительным местом на Земле».

За некоторую сумму кто угодно мог скачать с сервиса изображения. Изображения были из тех, которые не принято показывать в приличном обществе, но которые можно увидеть в журналах, продаваемых в городах Сан-Франциско и Сан-Хосе. Создателями сервиса заинтересовалась полиция Сан-Хосе, сотрудники которой сочли, что сервис распространяет непристойные материалы. После изучения изображений полицейские решили, что – по местным стандартам – изображения не являются непристойными.

Разработчикам сервиса не было предъявлено обвинение, так что на электронной доске появилось следующее сообщение: «Полицейское управление Сан-Хосе, окружная прокуратура Санта-Клара и правительство штата Калифорния подтверждают, что электронная конференция Amateur Action BBS действует в рамках закона».[1]

[1] Дэвид Лаунди (David Loundy) «Whose Standards? Whose Community?» (Чьи стандарты? Чьего общества?), *Chicago Daily Law Bulletin* от 1 августа 1994 года, *www.loundy.com/CDLB/AABBS.html*.

Два года спустя, в феврале 1994 года, создатели сервиса Amateur Action снова привлекли внимание полиции и их компьютер был изъят. Основанием явилось заявление от агента Дэвида Дирмайера, почтового инспектора *с запада штата Теннесси*. Под вымышленным именем инспектор заплатил сервису 55 долларов и скачал набор изображений на свой компьютер в Мемфисе. Содержимое представлялось отвратительным, особенно для Мемфиса: зоофилия, кровосмешение и садо-мазохизм. Создатели сервиса были арестованы и предстали перед судом Мемфиса по обвинению в распространении непристойных материалов с применением общедоступных средств передачи, а также в торговле между штатами. Судья штата Теннесси вынес обвинительное заключение о том, что расположенная в Мильпитасе электронная доска объявлений нарушила общественные нормы Мемфиса. Судья установил сроки тюремного заключения: Боб – 37 месяцев, Карлин – 30 месяцев.

Обвиняемые обжаловали приговор на том основании, что не могли знать, куда будет направлен поток битов, и что сообщество пользователей конференции принадлежит не Сан-Хосе, а Киберпространству. Апелляционный суд отклонил аргументы защиты: инспектор Дирмайер при вступлении в собщество пользователей предоставил почтовый адрес, принадлежащий штату Теннесси, создатели сервиса звонили инспектору в Мемфис, чтобы сообщить пароль для доступа, следовательно, знали местонахождение абонента. Создателям сервиса Amateur Action, по мнению судьи, необходимо более внимательно определять, куда они отправляют биты, тем более что отправка осуществляется за пределы штата. Передача битов примерно то же самое, что почтовая пересылка видеокассет (что также являлось одним из пунктов обвинения). Законы реального мира сработали в Киберпространстве, и правовые стандарты одного города вдруг оказались действительны на расстоянии в несколько тысяч километров.[1]

Самая демократичная форма массового общения

Порнография стала частью электронного мира с того момента, как появилась возможность хранить и передавать слова и изображения. Боб и Карлин Томас смогли на собственном печальном примере убедиться, что биты подобны книгам в смысле применения стандартов пристойности.

В середине 1990-х произошло еще кое-что. Распространение компьютеров и вычислительных сетей значительно увеличило количество доступных цифровых изображений и тех, кто их просматривает. Цифровая порнография стала не просто новой формой старого явления, а чем-

[1] «Федеральный апелляционный суд США против Роберта Алана Томаса и Карлин Томас», 1996 FED App. 0032P (6th Cir.), решение принято 29 января 1996 года, *www.epic.org/free_speech/censorship/us_v_thomas.html*.

то совершенно новым, потому что порнографии стало много, и ее стало легко достать и пронести домой. Сенатор от штата Небраска Джеймс Эксон предложил поправку о запрете электронной порнографии к закону о телекоммуникациях, но поправка оказалась изначально обречена на поражение. А затем ад вырвался наружу.

3 июля 1995 года журнал «Time Magazine» вышел с надписью «Киберпорнография» поперек обложки. Соответствующая статья, основанная главным образом на университетском отчете, сообщала:

> *Исследователи университета Карнеги-Меллон обнаружили: В СЕТИ ЧУДОВИЩНОЕ КОЛИЧЕСТВО ПОРНОГРАФИИ. В течение 18 месяцев группа исследователей обнаружила 917 410 изображений, описаний, коротких рассказов и видеозаписей сексуального характера. В группах новостей Usenet, где хранились цифровые изображения, 83,5% изображений являются порнографией.*[1]

Далее в статье пояснялось, что статистика охватывала лишь небольшую выборку всего потока данных. Не было упомянуто, что непристойные изображения хранились в основном на закрытых сервисах, не доступных детям и большинству взрослых людей. Статья отмечала необходимость правительственной цензуры и цитировала слова Джона Барлоу о важной роли родителей. Тем не менее, когда сенатор Грэсли от штата Айова увидел в копии статьи в «Congressional Record» – официальном бюллетене заседаний законодательной власти – подтверждение результатов исследований, проведенных факультетом права университета Джорджтауна, он обратился к Конгрессу с призывом «помочь родителям детей, которые в это время и в этом возрасте уже находятся в смертельной опасности» и «помочь остановить нарастающий поток».

Речь сенатора Грэсли и примеры непристойных изображений, найденные другом сенатора Эксона, заставили Конгресс действовать во имя спасения детей Америки. В феврале 1996 года Акт о пристойности в коммуникационных сетях прошел почти единогласно и был подписан президентом Клинтоном.

Акт объявил преступлением использование «какого бы то ни было интерактивного компьютерного сервиса, чтобы воспроизводить способом, доступным лицу, не достигшему 18 лет, какие бы то ни было комментарии, запросы, предложения, заявки, изображения или иные ресурсы, которые в данных условиях изображают или описывают в терминах явно непристойного характера, как отмечено действующими общественными нормами, половые или экскреторные действия или органы». Уголовному преследованию также будут подвергнуты те, кто «сознательно разрешает какую бы то ни было коммуникационную активность под контролем вышеозначенных лиц». И наконец, акт объяв-

[1] Филип Элмер-ДеВитт (Philip Elmer-DeWitt) «On a screen near you» (На экране перед вами), *Time Magazine* от 3 июля 1995 года.

ляет уголовным преступлением передачу «непристойных или неприличных» материалов лицам, явно не достигшим 18 лет.

Описанные в акте «ограничивающие положения» существенно расширили существующее законодательство по борьбе за общественную мораль, которое уже применяется для регулирования деятельности в Интернете. Двойные запреты – против *предоставления доступа* и *доставки непристойных материалов* лицам, явно *не достигшим 18 лет*, – отличались от всех норм, когда-либо применяемых в отношении печатных изданий. «Неприличие», что бы это ни значило, явно не является непристойностью; а до принятия Акта о пристойности в коммуникационных сетях были нелегальны только непристойные материалы. Продавец в уличном киоске может отличить 12-летнего покупателя от 20-летнего, но как можно узнать истинный возраст в Киберпространстве?

После принятия акта Джон Барлоу оценил потенциал Интернета для свободного распространения любой нужной информации. Джон Барлоу выпустил ставший классическим манифест, направленный против усилий правительства по контролю свободы слова:

> Правительства Мира индустрий, уставшие гиганты из плоти и стали, я пришел из Киберпространства, нового дома Разума. Ради будущего я прошу вас, принадлежащих прошлому, предоставить нас самим себе. Там, где мы собираемся вместе, у вас нет власти... Мы создаем мир, в который может войти каждый, не имея привилегий или преимуществ, создаваемых цветом кожи, экономической или военной силой или местом рождения. Мы создаем мир, в котором кто угодно и где угодно может исповедовать свои убеждения независимо от их необычности, без страха быть принужденным к молчанию или согласию... В нашем мире все отношения и выражения человечества, от развращающих до ангельских, являются частями единого целого, глобального обмена битами... <Вы> пытаетесь ограничить распространение вируса свободы путем установки караульных постов на границах Киберпространства.[1]

Это смелые и дерзкие слова, даже если учесть, что понятие Киберпространства как «единого целого» уже взято под сомнение. Как минимум, биты должны соответствовать нормам пристойности места назначения, в чем уже убедились создатели сервиса **Amateur Action. В сущности,** понимание Интернета как «пространства», имеющего «границы», является фатальной ошибкой, и это ошибочное понимание продолжает преследовать законы и политики до настоящего времени.

К хору голосов, направленных против Акта о пристойности в коммуникационных сетях, присоединились борцы за гражданские права. Федеральный и Верховный суды в упрощенном порядке рассмотрели дело

---

[1] Джон Перри Барлоу (John Perry Barlow) «A declaration of the independence of Cyberspace» (Декларация независимости Киберпространства), 8 февраля 1996 года, *homes.eff.org/~barlow/Declaration-Final.html*.

«Американский союз гражданских свобод против Рено». «Ограничивающие положения» акта оказались противоречащими Конституции США. «Правительство может ограничивать свободу слова только по причинам исключительной важности, – отметил в решении председатель окружного суда Дэлзелл, – и только способом, в наименьшей степени ущемляющим права». Будет считаться явно недопустимым требовать через Интернет подтверждения возраста от каждого, у кого есть возможность увидеть материалы, видеть которые имеет законное право любой совершеннолетний гражданин.

Правительство выдвинуло возражение о том, что право Федеральной комиссии по коммуникациям управлять содержанием тех теле- и радиопередач, которые должны быть «пристойными», предоставляет аналогичное право правительственного надзора за Интернетом.

Суды отвергли предложенную аналогию: Интернет – более открытая система, чем кабельное или эфирное вещание. Различные средства получения информации требуют разного законодательного подхода, поэтому законы о ТВ и радио имеют более широкий круг ограничений, чем были для печатных изданий или должны быть – для Интернета. «Я не сомневаюсь, – писал судья Дэлзелл, что Акт о пристойности в газетных изданиях (Newspaper Decency Act), принятый потому, что Конгресс обнаружил, как много юных девушек прочли передовицу «New York Times» об обрезании женщин в Африке, может быть сочтен неконституционным... Интернет определенно может рассматриваться, как нескончаемый всемирный разговор. Правительство не может прервать этот разговор одним лишь Актом о пристойности в коммуникационных сетях. Как наиболее демократичная форма массового общения из когда-либо созданных, Интернет заслуживает самого высокого уровня защиты от правительственного вмешательства».[1] Ограничения акта оказались непригодными.

В сущности, суд не желал приносить потенциал Интернета как обширного рынка идей в жертву узкой цели защиты детей от непристойностей. Вместо этого суд переложил обязанность по блокированию нежелательных коммуникаций с интернет-провайдеров на принимающую сторону. Предполагаемый Актом об удалении сетевых хищников контроль библиотек и школ – прямое следствие судебных постановлений, отвергающих положения Акта о пристойности в коммуникационных сетях. С точки зрения закона, контролировать содержимое потока битов можно только в той точке, в которой биты выходят из «облака» и передаются приемнику.

В истерии, разыгравшейся вокруг непристойности в Интернете в 1995–1996 годах, забылось то, что «Отчет университета Карнеги-Меллона», с которого начался снежный ком новых законов, оказался дискреди-

[1] Гражданское дело «ACLU против Рено», № 96-963, суд Восточного округа штата Пенсильвания, 12 июня 1996 года.

тирован почти сразу после публикации в журнале «Time Magazine». Автор отчета Мартин Римм был выпускником по специальности инженер-электрик. Методология исследования содержала ошибки и, возможно, данные были подтасованы. Как стало известно, Мартин Римм говорил операторам сетевых конференций для совершеннолетних посетителей, что исследует новые приемы продажи порнографии в Интернете, и предлагал свою помощь за плату. Выводы отчета не были надежными. Почему это не сообщили сразу после публикации статьи? Потому что статья не была «публикацией университета Джорджтауна», как заявил сенатор Грэсли. Статья появилась в «Georgetown Law Review» – студенческом издании, где не было ни собственных, ни профессиональных рецензентов. Спустя три недели после выхода статьи «Киберпорнография» редакция журнала «Time Magazine» признала, что отчет Мартина Римма не являлся надежным источником. Несмотря на это опровержение, студент был вознагражден за свои усилия: он опубликовал книгу – руководство по зарабатыванию денег на распространении порнографии («The Pornographer's Handbook: How to Exploit Women, Dupe Men, & Make Lots of Money»[1]).

Защита электронных прав и свобод

Фонд электронной безопасности – это ведущая общественная организация правозащитников, отстаивающих положения Первой поправки и другие права личности в Интернете. Как ни странно, фонд часто оказывается в оппозиции к вещательным и телекоммуникационным компаниям. В принципе, последние должны быть больше всех заинтересованы в неограниченном распространении информации. В реальности, компании нередко получают доход от политики ограничений или отслеживаний частных потребителей. Фонд электронной безопасности был среди истцов, возбудивших дело, которое лишило силы Акт о пристойности в коммуникационных сетях.

Защита добрых самаритян... и некоторых злых

Решение по делу «Stratton Oakmont против Prodigy», которое отбило у интернет-провайдеров всякую охоту вводить цензуру содержимого, было вынесено в 1995 году, как раз в то время, когда Конгресс готовился утвердить Акт о пристойности в коммуникационных сетях, чтобы защитить детей от порнографии в Интернете. Конгрессмены осознали,

[1] *Casino Forum*, март 1995 года.

что одним из последствий решения по упомянутому делу будет низкое сопротивление провайдеров размещению сайтов с непристойным содержимым. Поэтому инициаторы акта добавили в акт положение о «добрых самаритянах».

Исключение было добавлено, чтобы позволить провайдерам действовать в качестве редакторов, не навлекая на них риск понести ответственность за содержимое сайтов, и, таким образом, исключить возможность испытать на себе все «прелести» печального положения, в котором оказался сервис Prodigy. Новое положение Акта позволило провайдерам фильтровать информацию, оставаясь в рамках закона, и с благой целью удаления «непристойных, распутных, вызывающих похоть, грязных, исключительно насильственных, отталкивающих и тому подобных» материалов. Для примера в Акт было помещено определение «распространителя», как оно понималось при рассмотрении дела «Cubby против CompuServe». Не следовало рассматривать поставщиков услуг компьютерной связи как издателей или как первоначальные источники информации. «Ни один провайдер или пользователь не должен считаться издателем или источником какой бы то ни было информации, поставленной иным распространителем содержимого».[1] Это было заключительное предложение параграфа 230 Акта о пристойности в коммуникационных сетях, и оно означало, что больше никто не попадется в такую ловушку, как «Stratton Oakmont против Prodigy».

Когда Верховный суд США в 1996 году отклонил проект Акта о пристойности в коммуникационных сетях, причиной отклонения были лишь ограничивающие положения документа, предусматривавшие наказание поставщиков «непристойного» содержимого. Положения о «добрых самаритянах», однако, прошли рассмотрение и остаются законом по сей день. Провайдеры могут неограниченно фильтровать или подвергать цензуре содержимое сайтов без какого бы то ни было риска судебного преследования издателями.

Или же провайдеры могут вовсе не редактировать содержимое, в чем убедился к своему горю Кен Зеран несколько лет спустя.

Акт о пристойности в коммуникационных сетях и дискриминация

Определение «добрых самаритян» провело четкую границу между поставщиками услуг компьютерной связи (не несущими ответственности) и «распространителями содержимого» (несущими ответственность). С расширением мира технологий граница стала менее четкой. Один из чатов (сервис комнат интерактив-

[1] Акт о пристойности в коммуникационных сетях, § 230(c) (1, 2).

ного сетевого общения), расположенный в штате Калифорния, был вынужден защищаться в суде по обвинению в насаждении пользовательской дискриминации (комнаты только для женщин, к примеру). Суд постановил, что операторы веб-сайта сервиса являются поставщиками услуг и не несут ответственности. Апелляционный суд вынес обратное решение на основании того, что сайт, фильтруя (если вы ищете комнаты общения «только для женщин», то не узнаете о пользователях мужского пола) информацию, размещаемую пользователями, переходит в категорию поставщиков содержимого. Здесь не было ошибки, однако при том, что *право фильтрации сервиса было защищено законодательством*, оно же позволяло равно безнаказанно распространять и поддерживать расовые или иные преференции. Такая форма разделения в газетных изданиях является противоправной. «Мы сомневаемся, – писал председатель апелляционного суда, – что это именно то, что Конгресс имел в виду при принятии Акта о пристойности в коммуникационных сетях».[1]

Самый крупный теракт на территории США до разрушения Всемирного торгового центра в Нью-Йорке 11 сентября 2001 года – это взрыв здания федерального правительства им. Альфреда П. Мурра в Оклахома-Сити 19 апреля 1995 года. При взрыве погибли 168 человек, в том числе несколько детей. Еще несколько сотен получило ранения от осколков строительных материалов при разрушении здания. Один из выживших сравнил происходящее со взрывом атомной бомбы.[2]

Меньше чем через неделю после теракта некто под псевдонимом «Ken ZZ03» разместил рекламное объявление на электронной доске объявлений сервиса America On Line (AOL). Для продажи предлагались «Рисковые футболки из Оклахомы». Среди доступных надписей на футболках предлагались такие: «Посетить Оклахому – это взрыв!» и «Сомни, сваляй и упакуй их – Оклахома'95». Другие лозунги были еще отвратительнее. Заказать футболки предлагалось по указанному номеру телефона.

Номер принадлежал Кену Зерану, артисту и кинорежиссеру из Сиэттла (Вашингтон). Мистер Зеран не размещал злополучное объявление. Это была чья-то злая шутка.

Спустя какое-то время начали приходить звонки. Гневные, осуждающие звонки. Потом смертельные угрозы.

---

[1] Дело «Совет добропорядочных домовладельцев долины Сан-Фернандо против Roommates.com», №№ 04-56916, 04-57173, апелляционный суд, 15 мая 2007 года.

[2] *www.cnn.com/US/OKC/daily/9512/12-30/index.html*

Мистер Зеран позвонил в службу поддержки AOL и попросил удалить сообщения и составить опровержение. Оператор службы поддержки пообещал удалить сообщение, но составление опровержений противоречило политике компании.

На следующий день неизвестный пользователь под слегка измененным псевдонимом снова начал предлагать футболки с еще более отвратительными заголовками.

«Позвоните Кену. Кстати, спрос высок. Если телефон занят, звоните снова».

Мистер Зеран повторно обратился в службу поддержки AOL, чтобы попросить удалить текущие сообщения и предотвратить появление новых. Работники сервиса пообещали выполнить просьбу, но не сдержали обещания. К концу апреля мистеру Зелану приходили звонки каждые две минуты. Бизнес режиссера зависел от этого номера – если сменить номер или не брать трубку, то можно лишиться средств к существованию.

В это время Шеннон Фуллертон, ведущий утреннего радиошоу на станции KRXO в Сиэттле, получил сообщение электронной почты с копией одного из сообщений о продаже футболок. Обычно шоу представляло собой веселую болтовню, но после теракта несколько выпусков было посвящено трагедии в Оклахома-Сити. Ведущий зачитал слоганы из сообщения в эфире, прибавил телефонный номер и попросил слушателей «позвонить Кену» и сказать предпринимателю все, что они о нем думают.

Должна ли радиостанция нести ответственность?

Кен Зеран подал отдельный иск против радиостанции, но и здесь не преуспел. Нанесенный ущерб не был следствием клеветы со стороны радиостанции, так как никто из звонивших даже не знал, кем на самом деле был человек на другом конце провода. Поэтому негативные высказывания ведущего радиошоу в адрес «Кена» скорее всего не нанесли ущерба репутации Кена Зерана – таково было решение суда.[1]

Режиссер получил еще больше звонков и смертельных угроз. Опасаясь за свою жизнь, мистер Зеран договорился с полицией об охране своего дома. Большинство звонивших не интересовалось тем, что им могли

[1] Дело «Зеран против Diamond Broadcasting», апелляционный суд, №№ 98-6092, 98-6094, принято в производство 28 января 2000 года, *legal.web.aol.com/decisions/dldefam/zerandia.html.*

ответить, однако режиссер услышал достаточно, чтобы узнать о радиошоу Шеннона Фуллертона. Режиссер созвонился с радиостанцией и убедил руководство сообщить в эфире о непричастности к объявлениям. После выхода опровержения число «звонков Кену» сократилось примерно до 15 в день. В конце концов, некая газета сообщила о том, что объявления были ложными. Сервис AOL наконец-то (после недельной видимости) удалил рекламные сообщения. Жизнь Кена Зерана начала возвращаться в нормальное русло.

Режиссер подал иск против компании AOL по обвинению в клевете, помимо прочего. Размещая рекламные сообщения и сохраняя их долгое время после получения сведений об их ложности, компания AOL причинила Кену Зерану серьезный ущерб.

Решение суда оказалось в пользу компании AOL, и иск был передан в апелляционный суд. Компания AOL определенно могла считаться издателем, так как разместила рекламные объявления и не удалила их после того, как они были признаны ложными. В отличие от ответчика по делу «Cubby против CompuServe», компания AOL точно знала, что именно публикует. Однако защита «добрых самаритян», созданная Актом о пристойности в коммуникационных сетях, *сняла* с компании ярлык издателя вместе с ответственностью.

Единственным положительным моментом (и шансом на возмещение ущерба) для режиссера могло бы стать установление личности, скрывавшейся под псевдонимом «Ken ZZ03». Но компания AOL не желала помочь. Никто не мог предложить Кену Зерану ничего, кроме сочувствия.

Пользователи могут избежать ответственности, оставаясь анонимными, что было легко сделать в Интернете. А Конгресс предоставил провайдерам полную индульгенцию – даже в случае осведомленности о размещении явно ложных сведений. Понимал ли хоть кто-нибудь в Конгрессе полный смысл положения о «добрых самаритянах»?

Законы с непредусмотренными последствиями

Положения о «добрых самаритянах» Акта о пристойности в коммуникационных сетях являются друзьями свободы слова и великим облегчением работы для интернет-провайдеров. Но применение Акта пошло вразрез с принципами, по которым он был создан.

Сидни Блюменталь был помощником президента Клинтона. Обязанностью помощника было поливать грязью врагов хозяина. 11 августа 1997 года консервативный сетевой обозреватель Мэтт Драдж написал: «В прошлом Сидни Блюменталя есть факты жестокого обращения с супругой, но это тщательно скрывается». Белый дом опроверг это заявление, и на следующий день обозреватель взял свои слова назад. Супруги Блюменталь подали иск к компании AOL, которая имела

Положение о «добрых самаритянах» Акта о пристойности в коммуникационных сетях в свое время помогло уйти от ответственности провайдеру, в одном из чатов которого продавалась детская порнография.

дело с мистером Драджем. И у которой был глубокий карман: истцы запросили 630 000 021 доллар возмещения. Супруги Блюменталь заявили, что компания AOL должна нести ответственность, как и обозреватель, потому что компания могла бы отредактировать его тексты. Ответчик настаивал, что обозреватель удалил часть текста по просьбе компании. Судья принял сторону ответчика и процитировал положения о «добрых самаритянах».[1] Компания AOL была освобождена от ответственности за слова обозревателя, так как не являлась издателем. Дело было закрыто.

Еще более поразительно то, что положение о «добрых самаритянах» в свое время помогло уйти от ответственности провайдеру, в одном из чатов которого продавалась детская порнография.

В 1998 году некая женщина и ее младший сын подали в суд на компанию AOL за причинение вреда сыну. Истцы заявили, что в чате на сайте AOL продаются порнографические снимки мальчика, сделанные, когда ему было 11 лет. Фотографии были сделаны неким Ричардом Ли Расселом, который завлек трех мальчиков с целью участия в совместных сексуальных действиях. Позже Ричард Рассел стал продавать порнографические фотографии и видеозаписи в чате.

Поэтому семья подала иск на компанию AOL. В соответствии с пользовательским соглашением компания вправе остановить обслуживание любого пользователя, замеченного в подобной деятельности. Но компания не только не пресекла торговлю Ричарда Рассела, но даже не предложила ему прекратить свои действия. Истцы требовали от ответчика компенсации за пособничество торговцу.

Дело было решено в пользу провайдера. Суд освободил компанию AOL от ответственности на основании положения о «добрых самаритянах» и прецедента Кена Зерана. Поставщики услуг электронных конференций и досок объявлений могут быть наказаны за распространение детской порнографии, только если сами рекламируют этот товар.

Рассмотрение иска в апелляционном суде также завершилось не в пользу потерпевших. Верховный суд штата Флорида принял решение голосованием четырех судей против и трех за удовлетворение иска. Судья Дж. Льюис открыто высказал свое несогласие с общим решением. По мнению судьи Льюиса, положение о «добрых самаритянах» было направлено против добросовестных участников, разрабатывающих технологии блокирования и фильтрации данных, которые могли бы быть

[1] «Сидни Блюменталь и Жаклин Джордан Блюменталь против Мэтта Драджа и America Online», гражданское дело № 97-1968, суд округа Колумбия, 22 апреля 1998 года, *www.techlawjournal.com/courts/drudge/80423opin.htm*.

использованы родителями для защиты детей. «Совершенно невозможно допустить, чтобы Конгресс при разработке Акта о пристойности в коммуникационных сетях руководствовался намерением оободить от ответственности тех провайдеров, которые не предпринимают никаких мер даже против явно противозаконных действий пользователей... в то же время продолжая наживаться на предоставлении услуг связи». Закон превратился в средство «прощения и реабилитации возмутительного и достойного осуждения бездействия провайдеров при виде... материала, безусловно вредоносного для детей». Это не возымело никакого эффекта. Последовательность решений «отбросила Конгресс на недопустимую позицию, в которой он принял закон, потворствующий и защищающий молчаливое согласие провайдеров и их соучастие в создании преступных предприятий».[1]

С точки зрения судьи Льюиса, проблема заключалась в том, что было недостаточно объявить провайдеров «не-издателями». Провайдеры фактически являются чем-то большим, чем распространители, – что пытался доказать режиссер Зеран, – а даже распространители *не всегда* освобождаются от ответственности за свою деятельность. Водитель грузовика, если он знает, что возит детскую порнографию, и получает долю от прибыли, несет и свою долю правовой ответственности за соучастие в нелегальной торговле. Водитель не является издателем, но также является чем-то большим, чем просто перевозчик. Суд по иску режиссера породил неразбериху, использовав ошибочную аналогию. Конгресс усилил хаос, объявив аналогию издателя неверной, но не предложив альтернативы.

Можно ли считать Интернет журнальным киоском?

После признания в 1997 году ограничивающих положений Акта о пристойности в коммуникационных сетях противоречащими Конституции Конгресс вернулся к работе над защитой детей Америки. Акт о защите детей в сети (Child Online Protection Act, COPA) получил статус закона в 1998 году. Этот акт взял многое от Акта о пристойности в коммуникационных сетях; сузив поле охвата, поскольку предполагалось избежать проблем с несоответствием Конституции США. Новый акт мог быть применен только к «коммерческим» проявлением гласности и налагал ответственность за предоставление несовершеннолетним «вредоносных материалов». «Несовершеннолетним» в данном случае считался человек, не достигший 17 лет. Закон также расширил тест Миллера для определения «материалов, вредоносных для несовершеннолетних», но не являющихся «непристойными»:

[1] «Джейн и Джон Ду против America Online», Верховный суд штата Флорида, 8 марта 2001 года, № SC94355, отказано Дж. Льюисом, *www.eff.org/legal/ISP_liability/CDA230/doe_v_aol.pdf*.

> Термин «материалы, вредоносные для несовершеннолетних» означает материалы, распространяемые по каналам связи... такие, что: а) вызывают в целом у среднестатического гражданина, следующего общепринятым стандартам, или, в частности, у несовершеннолетнего... похотливый интерес; б) изображают, описывают или символизируют явно оскорбительным образом, в частности, для несовершеннолетнего... половой акт или непристойное обнажение гениталий или сформировавшейся женской груди; в) имеют в целом отрицательную литературную, художественную, политическую или научную ценность для несовершеннолетнего.

Новый акт был немедленно подвергнут критике и никогда не применялся. Один федеральный судья порекомендовал правительству воздержаться от применения акта, так как обнаружил в тексте закона несоответствие Конституции. В течение двух президентских сроков этот вопрос рассматривался в судах. Дело началось под названием «Американский союз гражданских свобод против Рено», позднее было переименовано в «Американский союз гражданских свобод против Эшкрофта» и, наконец, – «... против Гонсалеса». Судьи обычно были на стороне Конгресса, стремясь защитить детей от материалов, которые несовершеннолетним видеть не следует. Но в марте 2007 года Акт о защите детей в сети был похоронен окончательно. Председатель окружного суда Восточного округа штата Пенсильвания Лоуэлл Рид-мл. подтвердил, что закон зашел слишком далеко в ограничении свободы слова.

Частично проблема заключалась в нечетком определении «материалов, вредоносных для несовершеннолетних». Интимные интересы шестнадцатилетних и восьмилетних нельзя назвать одинаковыми; то же верно и в отношении литературных интересов. Как может разработчик веб-сайта действовать, не зная стандартов, которым нужно следовать, чтобы избежать риска тюремного заключения?

Есть и более фундаментальная проблема. Акт о защите детей в сети полностью посвящен тому, как избежать попадания определенных материалов в руки детей, в то время как эти же материалы совершенно законно могут хранить совершеннолетние граждане. Акт создал необходимость распространителям информации проверять возраст пользователей. Для тех, кто с благими намерениями осуществлял меры по проверке истинного возраста, акт обеспечил «тихую гавань». Конгресс использовал аналогию с журнальным киоском: продавец не должен продавать непристойные журналы лицам, не достигшим порогового возраста, и может потребовать доказательств от тех, кто выглядит несовершеннолетним. Закон представил нечто подобное в Интернете:

> Определенной защитой от преследования в данном случае является факт того, что ответчик с благими намерениями ограничил доступ к материалам, вредоносным для несовершеннолетних, путем:

а) требования использования кредитной карты, дебетного счета, кода доступа или персонального идентификационного номера совершеннолетнего; б) получения цифрового сертификата, удостоверяющего возраст; в) введения любых иных доступных на данном уровне развития технологии средств.

Но указанные «средства» в настоящее время либо неэффективны, либо еще даже не разработаны. Не каждый совершеннолетний пользуется кредитными картами, а компании не желают, чтобы их базы данных о клиентах использовались для проверки возраста. И если вы не знаете, что означают слова «персональный идентификационный номер совершеннолетнего» или «цифровой сертификат, удостоверяющий возраст», то не обвиняйте себя в отсталости – мы этого тоже не знаем. Пункты «б» и «в», в сущности, являются попыткой Конгресса сослаться на промышленность, которая вдруг придет и покажет некие волшебные технологии определения возраста на расстоянии.

В настоящее время компьютеры не способны точно установить, человек ли оператор конечного узла – или другой компьютер. Установить с помощью компьютера, является ли собеседник совершеннолетним, хотя бы приближенно, также почти невыполнимая задача. Бесшабашные пятнадцатилетние подростки способны справиться с любой системой контроля доступа, которую можно установить в обычном доме. Интернет – это все-таки не журнальный киоск.

Судья Рид также полагал, что, хотя использование кредитных карт или персональных идентификационных номеров поможет отделить детей от взрослых, оно же отпугнет пользователей компьютеров. Страх перед кражей персональных данных или установлением правительственного надзора может заставить пользователей отказаться применять идентифицирующую информацию, чтобы зайти на сайт, считающийся «вредоносным для несовершеннолетних». На практике это означает, что колоссальная электронная библиотека перестанет пользоваться прежней популярностью и на ней можно будет поставить крест, как и на обычной библиотеке, которая станет бесполезной, когда каждый, кто вырос из детской секции, должен будет проходить проверку.

В заключение судья Рид отметил, что рекомедации Конгресса по контролю за содержимым сайтов при их воплощении в жизнь существенно ограничат свободу слова в Интернете. Информация, которую взрослые вправе получать в реальной жизни, станет для них недоступной. Со времени разработки проекта Акта о защите детей в сети упомянутые в нем технологии были усовершенствованы, поэтому теперь правительство не может безоговорочно заявлять, что ограничение свободы слова – единственное средство защиты детей. Даже если свобода слова будет ограничиваться или нарушаться, даже если все меры, указанные в Акте, будут работать совершенно, дети все еще смогут увидеть много грязи. Интернет не имеет границ, а сила акта ограничена территорией

Соединенных Штатов. Акт не сможет остановить поток вредоносных битов из-за границы.

Подводя итоги, судья Рид процитировал слова члена Верховного суда Кеннеди по делу о сжигании флагов: «Остается фактом, что иногда нам приходится принимать решения, которые нам не нравятся. Мы принимаем их, потому что считаем их правильными, в том смысле что Конституция и другие законы, как мы их видим, приносят нужный результат». До конца поддерживая идею защиты детей от возможного вреда со стороны средств массовых коммуникаций, судья Рид все же заявил: «Возможно, мы причиним вред несовершеннолетним гражданам нашей страны, если защита Первой поправкой свободы слова, которую они захотят обрести по достижении совершеннолетия, будет ослаблена во имя их собственной защиты».[1]

Преследование с помощью клавиатуры

Телеконференции по обмену сексуальными фантазиями и опытом появились в начале 1980-х. К середине 1990-х для каждой ориентации или склонности можно было найти свой сайт. Так что когда женщина 28 лет в 1998 году зашла в чат поделиться своими сексуальными фантазиями, в ее поведении не было ничего необычного. По словам женщины, ей нравилось подвергаться насилию, и она приглашала того, кто читал ее сообщения, воплотить эти фантазии в реальность. «Я хочу, чтобы ты выломал дверь и изнасиловал меня», – писала женщина.

Необычным было то, что женщина сообщала свои имя и адрес – а также инструкции о том, как преодолеть систему безопасности здания. За несколько недель приглашением воспользовались девять мужчин, как правило, появляясь перед ее дверью около полуночи. Отослав «гостя», она снова появлялась в чате, объясняя свой отказ все той же фантазией.

Как выяснилось, «женщиной», оставлявшей сообщения, был Гари Деллапента, пятидесятилетний охранник здания, чьи знаки внимания настоящая женщина решительно отвергала. У жертвы этой безумной «шутки» даже не было компьютера. Охранник был пойман, когда напрямую ответил на сообщение, отправленное, чтобы выследить злоумышленника. Он был арестован и осужден по недавно принятому в Калифорнии закону о противодействии интернет-травле (cyberstalking, киберсталкинг).[2] Дело было необычным не только из-за своей

---

[1] «ACLU против Гонсалеса», суд Восточного округа штата Пенсильвания, гражданское дело № 98-5591, окончательное решение, 22 марта 2007 года, *www.paed.uscourts.gov/documents/opinions/07D0346P.pdf*.

[2] «Computer stalking case a first for California» (Первое дело о компьютерном преследовании в штате Килифорния), *New York Times* от 25 января 1999 года; Валери Элворд (Valerie Alvord) «Cyberstalkers must beware of the e-law»

новизны, но также из-за того, что преступник был найден и наказан. Большинство жертв травли не могут добиться справедливости. Во многих штатах нет необходимой правовой базы, а жертва нередко не может опознать «охотника» (stalker, сталкер). Иногда сталкер даже не знаком с жертвой, а просто нашел ее контактные данные где-то в Киберпространстве.

Заявления и публикации, содержащие угрозы, в течение длительного времени оставались под защитой Первой поправки, особенно когда имели политическую направленность. Только когда сообщение было похоже на подготовку к «готовящемуся противоправному деянию» (фраза из решения Верховного суда 1969 года), текст становился противозаконным, что редко случалось с печатным словом.[1] Этот высокий порог правительственного вмешательства только в случае «явной и реальной опасности» наиболее ясно выражен в словах судьи Луи Брандье, опубликованных в 1927 году. «Опасение причинения серьезного ущерба не может само по себе служить основанием для подавления свободы слова... Никакая опасность, источником сведений о которой является речь, не может быть признана явной и существующей в действительности до тех пор, пока распространение осознанного зла не является настолько близким, что оно может обрушиться на будущих жертв еще до того, как повится возможность полноценного рассмотрения».[2]

Те же принципы судьи применяют к веб-сайтам. Группа сторонников запрещения абортов разместила списки имен, адресов и номеров лицензий врачей, проводящих аборты, на веб-сайте под названием «Нюрнбергские картотеки». Предполагалось «травить» врачей и обновлять сайт, помечая имена раненых серым цветом и зачеркивая имена убитых. Создатели сайта знали, что аборты разрешены законом, и заявляли, что не собираются никому угрожать, а просто коллекционируют досье в надежде на то, что когда-либо в будущем указанные медики будут осуждены за «преступления против человечества». Участники группы предстали перед судом по гражданскому иску. После долгого рассмотрения суд решил, что ответчики должны возместить ущерб, так как «реальные угрозы совершения насилия имели целью запугивание потерпевших».

Судьи встретились со значительными трудностями при определении того, является ли веб-сайт «Нюрнбергские картотеки» источником угрозы, хотя трудность заключалась вовсе не в способе опубликования данных. Та же группа активистов выпустила бумажные плакаты «В розыске», содержавшие часть материалов сайта. Юристы обосно-

(Киберсталкеры должны остерегаться электронных законов), *USA Today* от 8 ноября 1999 года.

[1] Дело «Бранденбург против штата Огайо», 395 U. S. 444 (1969).

[2] Дело «Уитни против штата Калифорния», 274 U.S. 357, 375–76 (1927). Судья Холмс поддерживает это решение.

ванно могли сделать (и делали) противоречащие друг другу заключения о том, подпадали ли тексты, опубликованные на сайте, под ту или иную правовую категорию.[1]

Ситуации с жертвой преследования со стороны охранника Гари Деллапента и подобными ей с точки зрения закона выглядят иначе. Эти дела не имели политической подоплеки. Уже существовали законы о противодействии интернет-травле и телефонному преследованию; набор волонтеров-сталкеров и людей, готовых совершать звонки, происходил посредством Интернета. Следуя примеру Калифорнии и нескольких других штатов, Конгресс принял федеральный закон о противодействии интернет-травле.

Всего лишь досаждающий телефонный звонок?

Акт о насилии в отношении женщин и изменении полномочий Департамента юстиции 2005 года (Violence Against Women and Department of Justice Reauthorization Act), вступивший в силу в начале 2006 года, подвергает уголовному преследованию каждого, кто «применяет любое аппаратное или программное обеспечение, с помощью которого можно создавать телекоммуникации или иные типы связи, частично или полностью использующие Интернет для передачи данных... скрывая свою личность и с намерением досаждать, оскорблять, угрожать или лишать покоя другое лицо...» Это положение при слушаниях в Палате представителей прошло открытым, а в Сенате – тайным голосованием.

Защитники гражданских свобод снова подняли шум, на этот раз из-за единственного не понравившегося слова. Они не были против выражения «оскорблять, угрожать или лишать покоя». Подобные действия имели свою правовую историю, хотя не всегда было легко сказать, соответствуют ли определения фактам, – по крайней мере, у судей были стандарты, которыми можно было руководствоваться.

Но вот «досаждать»? На веб-сайтах полно досаждающего содержимого, а в комнатах для бесед говорится много досаждающих слов. Есть даже сайт *annoy.com*, целиком посвященный анонимному размещению досаждающих политических сообщений. Неужели Конгресс действительно намеревался запретить использование Интернета из-за того, что он «досаждает» людям?

---

[1] Рене Санчес (Rene Sanchez) «Abortion foes' Internet site on trial; Doctors' fear of violence collides with radical opponents' rights to free speech» (Сайт противников абортов перед судом; страх врачей перед насилием против права радикально настроенных оппонентов на свободу слова), *Washington Post* от 15 января 1999 года; дело «Planned Parenthood of the Columbia/ Willamette Inc. и др. против Американской коалиции активистов жизни и др.», апелляционный суд, № 04-35214, 422 F.3d 949. Решение принято 6 сентября 2005 года.

Конгресс расширил область действия законов об использовании телефонной связи на Интернет, основываясь на том, что беспокоящие звонки интернет-телефонии не должны отличаться по степени наказания от обычных звонков. Однако, обобщив электронные коммуникации, Конгресс создал еще одну проблему с ошибочной метафорой.

Акт о телекоммуникациях 1934 года объявил преступником любого, кто использовал «телефонный звонок, независимо от того, состоялся ли диалог, не раскрывая свою личность, с намерением досаждать, оскорблять, угрожать или беспокоить любого человека, отвечающего по набранному номеру».[1] В области телефонии запрет не представлял угрозы свободе слова, так как телефонный разговор – это общение один на один. Если тот, с кем вы разговариваете, не желает слушать, то в этом нет никаких нарушений вашего права на свободу слова. Первая поправка не дает вам гарантии того, что вы будете услышаны. Если ваш звонок не приветствуется другой стороной, то можете досаждать кому-нибудь в другом месте. Акт о пристойности в телекоммуникационных сетях в положении, касающемся запретов, расширил их на факсимильную связь и электронную почту, по сути, являющиеся разновидностями общения один на один. Но в Акте о телекоммуникациях не было и не могло быть никаких упоминаний об интернет-телефонии и причинении ущерба с ее помощью. В попытке охватить одним положением закона все телефоноподобные средства коммуникации Акт о пристойности в телекоммуникационных сетях был распространен на все виды электронных коммуникаций, в том числе на обширную «электронную библиотеку» и «наиболее демократичную форму массового общения» – Интернет.

Сторонники усиления строгости законодательства заверили встревоженных авторов интернет-дневников, что «досаждающие» сайты не будут подвергаться преследованию со стороны закона до тех пор, пока сайты не станут также источниками персональных оскорблений, угроз или постоянного беспокойства. По словам законодателей, это были меры, направленные против кибертравли, а не против свободы слова. Первая поправка определенно останется в силе. Издатели электронных публикаций, напротив, неохотно поверили объяснениям представителей правосудия об области действия нового, расширенного закона. После множества фактов совершенно причудливого и неожиданного применения положения о «добрых самаритянах» не было никаких особых причин поверить в то, что подразумеваемый смысл нового акта сможет ограничить его формальное применение в определенной области Киберпространства.

Предложения по новому закону принимались в так называемый Ящик предложений (The Suggestion Box) – это служба, с помощью которой люди могут отправлять анонимные сообщения электронной почты, чтобы «сообщить важные сведения средствам массовой информации» или

[1] *www.dinf.ne.jp/doc/english/Us_Eu/ada_e/telcom_act/47/223.htm*

«способствовать раскрытию преступлений, информируя правоохранительные органы».[1] Недовольные новым законом приводили доводы о том, что акт может сделать преступниками тех работников-соглядатаев, которым Конгресс дал возможность вздохнуть с облегчением после серии скандалов с корпоративными деловыми практиками. Служба приема предложений отмела эти сомнения: федеральное правительство постановило, что противозаконным будет считаться только то использование средств коммуникации, которое «вызывает у жертвы страх». Итак, акт вступил в силу, сопровождаемый множеством пожеланий того, чтобы язык Конгресса на этот раз стал хоть немного более понятным.[2]

Что и возвращает нас в настоящее время. Положение о «досаждающих» осталось в Акте о насилии в отношении женщин, но лишь потому, что правительство объявило, что это слово означает нечто иное. Акт об удалении сетевых хищников, с которого началась эта глава, остается на доработке в Конгрессе. Как и Акт о пристойности в коммуникационных сетях или Акт о защите детей в сети, дорабатываемый законопроект имеет свои плюсы. Правда, предлагаемые актом меры могут принести больше вреда, чем пользы. Требование ввести надзор за посещением сайтов в библиотеках может сделать многие сайты недоступными, почти не причинив урона собственно «сетевым хищникам». Инициаторы законопроекта в Конгрессе поддались доброму порыву, но направили прогресс по ложному пути, пытаясь решить проблемы общества путем запрета полезной технологии.[3]

Цифровая защита, цифровая цензура и самоцензура

Запрет в Первой поправке на введение государственной цензуры осложняет работу этого самого государства по защите собственных граждан. Если придется выбирать между защитой от причинения личного ущерба и свободой некоего недоумка говорить все, что придет в голову, большинство людей выберет защиту. Безопасность приходит незамедлительно, свобода – понятие, требующее длительного времени для реализации преимуществ, а основная масса человечества мыслит краткосрочными категориями. Кроме того, большинство людей заботится только о собственной безопасности и охотно переложит на плечи правительства заботу о безопасности всей страны.

---

1 Дело «Suggestion Box против Гонсалеса». Цитируется по *www.theanonymousemail.com/*.

2 *TheAnonymousEmail.com* успешно получает ясное толкование федерального законодательства «о причинении раздражения» в деле против Генерального прокурора Гонсалеса и федерального правительства, *www.hotstocked.com/news/suggestion-box-inc-SGTB-4182764.html*.

3 RH 5319, 109 заседание Конгресса, 2 сессия, 27 июля 2006 года.

Если придется выбирать между защитой от причинения личного ущерба и свободой некоего недоумка говорить все, что придет в голову, большинство выберет защиту.

Но, по словам одного ученого, основным моментом Первой поправки можно считать, что «в обществе, предоставленном самоуправлению, никогда не может быть такого, что в долгосрочной перспективе безопасность нации окажется под угрозой из-за предоставления людям свободы».[1] Законы о вводе цензуры в Интернете прошли Конгресс главным образом потому, что конгрессмены не отважились записаться в число тех, кто голосует против безопасности избирателей – и особенно против защиты детей. Относительно свободные от политического давления судьи вновь и вновь отклоняют пропущенные выборными властями законопроекты, ограничивающие свободу слова.

Свобода слова – первая в списке прочих свобод, перечисленных в Билле о правах, но не только по номеру. Свобода слова логически предшествует остальным. Цитируя члена Верховного суда Бенджамина Кардозо, это «матрица, необходимое условие почти для всех прочих свобод».

В большинстве стран не так сильно беспокоятся по поводу ввода цензуры электронной информации.

Свобода в Интернете

Огромное число организаций прикладывают значительные усилия по поддержанию потенциала Интернета как свободного рынка идей. Кроме Фонда электронной безопасности, уже упомянутого в этой главе, среди участников движения: Информационный центр электронной конфиденциальности; Сеть свободного самовыражения (The Free Expression Network, *freeexpression.org*), в сущности являющаяся объединением организаций; Американский союз гражданских свобод; Центр анализа эффектов игнорирования тенденций (Chilling Effects Clearinghouse, *www.chillingeffects.org*). Проект OpenNet Initiative отслеживает случаи ввода цензуры в Интернете во всем мире. Сводка результатов опубликована в книге «Access Denied: The Practice and Policy of Global Internet Filtering» (Запрещенный доступ: практика и политика глобального интернет-фильтрования), составители Рональд Дж. Дейберт, Джон Г. Пэлфри, Рафаль Рогозински и Джонатан Зиттрейн (Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, Jonathan Zittrain).

[1] Александр Мейклджон (Alexander Meiklejohn) «Testimony on the Meaning of the First Amendment to the Senate Judiciary Subcommittee on Constitutional Rights» (Показания относительно значения Первой поправки сенатскому подкомитету по судопроизводству по конституционным правам), 1955.

В Саудовской Аравии нельзя зайти на сайт *www.sex.com*. Каждый запрос в Саудовской Аравии проходит через правительственные компьютеры – проверяется, не занесен ли адрес в «черный список». В Тайланде запрещен сайт *www.stayinvisible.com* – источник сведений об анонимности в Интернете и архив соответствующих программ.[1]

Несоответствие стандартов информационной свободы между США и другими странами создает конфликты при выполнении международных электронных стандартов. Как обсуждалось в главе 4, правительство Китая настаивало, чтобы поисковый сервис Google не предоставлял гражданам КНР возможность получать нежелательную с точки зрения государства информацию. Если вы попытаетесь из гостиницы в Шанхае получить доступ к определенным веб-сайтам, произойдет внезапный необъяснимый разрыв соединения. Можно даже подумать, что произошел сбой где-то в сети, но вы сможете повторно подключиться и без проблем посещать разрешенные сайты.

Самоцензура среди интернет-компаний встречается все чаще – это цена, которую приходится платить за присутствие их бизнеса в некоторых странах. Тайланд и Турция блокировали сайт хранения видеофайлов YouTube после того, как на нем появились видеозаписи, высмеивающие (и, с точки зрения правительств этих стран, оскорбляющие) нынешних или бывших глав государств. Один сотрудник корпорации Google описал интернет-цензуру как «барьер № 1 для торговли». Подстегиваемые возможными потерями в бизнесе и правовыми спорами, интернет-компании стали ярыми сторонниками информационной свободы, даже при том что им приходится следовать законам иностранных держав. Корпорация Google даже спонсирует своего лоббиста в Вашингтоне, чтобы обеспечить себе правительственную поддержку всемирного сопротивления контролю свободы слова.[2]

Американцам легко пожимать своими изоляционистскими плечами, глядя на эти проблемы. До тех пор пока в США доступна любая информация, – кого волнует, какая версия сервиса Google или YouTube доступна в одной из стран с тоталитарным режимом? Это их внутренние проблемы. Однако свободному потоку информации в США угрожают законы о регулировании средств массовой информации, действующие в других странах. Рассмотрим случай Джозефа Гутника и журнала «Barron's».

30 октября 2000 года финансовый еженедельник «Barron's» опубликовал статью о том, что австралийский бизнесмен Джозеф Гутник уличен в отмывании денег и уклонении от уплаты налогов.[3] Бизнесмен подал

---

[1] Примеры от OpenNet Initiative.

[2] Кристофер С. Ругабер (Christopher S. Rugaber) «Google ask feds to fight Internet censorship abroad» (Google просит федеральные власти бороться с цензурой в Интернете по всему миру), *Houston Chronicle* от 22 June 2007 года.

[3] Билл Альперт (Bill Alpert) «Unholy gains» (Нечестивые прибыли), *Barron's* от 30 октября 2000 года.

иск по обвинению в клевете издателя журнала – финансовой информационной компании Dow Jones. Иск был подан в австралийский суд. Джозеф Гутник считал, что интернет-издание журнала, доступное в Австралии за плату, аналогично печатному изданию. Компания выдвинула возражение, что местом «издания» является штат Нью-Джерси, где расположены ее веб-серверы. Следовательно, по мнению компании, дело должно рассматриваться в американском суде и по более либеральным в отношении прессы американским законам. Австралийский суд принял сторону истца.[1] Дело завершилось решением в пользу Джозефа Гутника: компания принесла извинения и выплатила 580 000 долларов штрафа и судебных издержек.[2]

Результат кажется ошеломляющим. Американцы на территории Америки считают, что могут изъясняться свободно. Однако австралийский суд решил, что Интернет распространил действие австралийских законов на территорию происхождения битов, достигших Австралии. Парадокс решения по делу сервиса Amateur Action о том, что стандарты отдельного сообщества могут быть применены в безграничном пространстве Интернета, был перенесен на всемирную прессу. Неужели свобода прессы в Интернете не сможет устоять даже перед самой малой страной на Земле? Возможно ли, что некая нация обманом будет вымогать у прессы огромные денежные суммы по обвинению в клевете или назначать смертную казнь журналистам, якобы оскорбившим лидеров держав?[3]

Американская пресса всеми силами отстаивает право публиковать правду, но проблемы цензуры в западных демократиях сильнее бьют даже не по прессе, а по транснациональным корпорациям. Иногда американской компании легче соответствовать минимальным «мировым» стандартам информационной свободы, чем обеспечивать доступность определенной информации в самой Америке. Международное право и торговые соглашения могут даже оказаться более удобными. Рассмотрим дело портала сервиса Yahoo! во Франции.

В мае 2000 года Международная лига борьбы с расизмом и антисемитизмом (Ligue Internationale Contre le Racisme et l'Antisemitisme) и Союз еврейских студентов Франции (Union des Opinion Etudiants

---

1 Верховный Суд Австралии, «Dow Jones and Co. против Гутника», HCA 56 (10 декабря 2002 года), *www.austlii.edu.au/au/cases/cth/high_ct/2002/56.html#fn204*.

2 «Gutnick settles suit» (Гутник выигрывает дело), *The Advertiser* от 12 ноября 2004 года.

3 Фелисити Бэррингер (Felicity Barringer) «Internet makes Dow Jones open to suit in Australia» (Интернет заставляет Dow Jones судиться в Австралии), *New York Times* от 11 декабря 2002 года; Уоррен Ричи (Warren Richey) «Once it's on the Web, whose law applies?» (Какие законы применять, когда предмет разбирательства оказывается в Интернете?), *Christian Science Monitor* от 19 декабря 2002 года.

Juifs de France) обратились во французский суд. Суть иска – требование запретить сервису Yahoo! предоставлять доступ на интернет-аукцион нацистской символике, показывать изображения нацистских реликвий и распространять антисемитские высказывания в доступных во Франции дискуссионных группах. В соответствии с французскими законами, запрещающими продажу и показ нацистских атрибутов, суд заключил, что корпорация Yahoo! нанесла оскорбление «коллективной памяти» страны и нарушила статью R654 Уголовного кодекса. Суд счел сервис Yahoo! угрозой «национальному общественному порядку» и потребовал от корпорации принять меры к тому, чтобы к указанным объектам нельзя было получить доступ на территории Франции.

Меры были приняты, и с французского портала Yahoo! (*yahoo.fr*) ссылки были удалены. Впоследствии сотрудники Лиги и Союза студентов обнаружили, что с территории Франции можно было попасть на американский портал сервиса – сайт *yahoo.com*. Подобно австралийскому суду, принявшему сторону местного истца, французский потребовал, чтобы оскорбительные объекты, изображения и фразы были убраны также с американского портала.

Какое-то время корпорация Yahoo! отбивала удары, заявляя, что не может знать, куда биты могут направиться, хотя этому заявлению трудно было поверить, учитывая то, что рекламные ссылки были на французском языке. В конце концов корпорация существенно пересмотрела свои стандарты для американского сайта. В соответствии с обновленными правилами сервиса расистские высказывания запрещались, а ссылки на нацистские реликвии исчезли. Но нацистские марки и монеты по-прежнему можно было продать на интернет-аукционе с американского сайта, так же как и копии «Mein Kampf». В ноябре 2000 года французский суд дополнил свое постановление: копии «Mein Kampf» не могут предлагаться для продажи на территории Франции. Штрафы возросли.

Корпорация Yahoo! обратилась за помощью к американским судьям. Корпорация настаивала, что по американским законам не совершила никакого преступления. Французские законы не могут пересечь Атлантику и оказаться сильнее законов США. Выполнение французского постановления может негативно отразиться на свободе слова в Америке. Окружной суд учел эти доводы и постановление было отменено заседанием трех членов апелляционного суда Северной Калифорнии.

Но в 2006 году на заседании в присутствии всех одиннадцати членов суд принял новое решение, на этот раз против корпорации. По мнению большинства корпорация была недостаточно наказана и предприняла слишком мало усилий по достижению компромисса с французской стороной, так что ссылки корпорации на Первую поправку не являются уместными. Мнения членов суда разделились только по поводу того, что делать дальше. «Мы не должны допускать, – писал судья Уильям

Флетчер, – чтобы решение иностранного суда могло быть использовано для отмены конституционной гарантии свободы слова».[1]

С увеличением числа битов, пересекающих национальные границы, подобные конфликты будут происходить все чаще. Будущий мир сформируют Законы, торговые соглашения, судебные постановления следующих лет, большинство из которых регулируют движение интеллектуальной собственности. Печальная ирония будет в том, что информационная свобода, так отчаянно защищаемая в США несколько столетий, в XXI веке выродится в комбинацию национальных законов о защите детей и интернациональных возможностей по заколачиванию денег. Но как сказал один британский комментатор, когда сервис размещения фотографий Flickr удалил часть файлов в соответствии с требованиями законодательства Сингапура, Германии, Гонконга и Кореи: «Свобода мысли и слова хороша, когда ты – хакер. Но бизнес есть бизнес».[2]

Печальная ирония будет в том, что информационная свобода, так отчаянно защищаемая в США несколько столетий, в XXI веке выродится в комбинацию национальных законов о защите детей и интернациональных возможностей по заколачиванию денег.

Свобода распространения информации в Интернете – это сложный бизнес. Технологии изменяются быстрее, чем закон успевает реагировать. Когда очередной скачок в развитий технологий начинает вызывать тревогу общественности, власти отвечают законами, чрезмерно упрощающими события. К тому времени, как новые законы становятся понятны и опробованы в судах, происходит очередной технологический скачок, и замедленный метаболизм законодательной системы пытается выдать запоздалую реакцию в виде нового плохо продуманного законопроекта.

Технологии теле- и радиовещания по-своему создают сенаторам проблемы. В мире массового вещания влиятельные силы бизнеса ратуют за законы об ограничении свободы слова, которые давно переросли породившие их технологии. Мы переходим к обзору изменений в мире радиоволн.

---

[1] Дело «Yahoo! Inc. против La Ligue Contree Le Racisme и др.», № 01-17424, D. C. № CV-00-21275,-JF, с. 505.

[2] Джон Нотон (John Naughton) «The Germans get their Flickrs in a twist over ‘censorship’» (Немцы используют свои записи в Flickr, для обхода «цензуры»), *The Observer* от 17 июня 2000 года.

Глава 8 | Биты в эфире

Старые метафоры, новые технологии и свобода слова

Цензура для президента

17 июля 2006 года, саммит стран «Большой восьмерки», Санкт-Петербург. Президент США Джордж Буш и премьер-министр Великобритании Тони Блэр спокойно беседуют. Сцена представляет собой отличный сюжет для съемки, но оба лидера и не подозревают, что микрофон включен. Президент и премьер-министр обсуждают возможные действия ООН по урегулированию конфликта между Израилем и вооруженными группами в Ливане. «Заметь иронию, – сказал президент, – что им нужно позволить Сирии договориться с Хезболлой остановить это shit, и все закончится».

Кабельная сеть CNN передала запись с места встречи в центр и разместила файл в Интернете[1], однако многие вещательные станции побоялись показывать это зрителям.[2] Никому не хотелось, чтобы Федеральная комиссия по коммуникациям (Federal Communications Commission, FCC) оштрафовала энтузиастов за появление в эфире слова «shit» (на сумму от 325 000 долларов).

FCC уже давно следит за соблюдением норм приличия в общественном эфире. В 2002 году, после церемонии награждения «Золотым глобусом», и без того строгие правила еще ужесточились. Певец Боно победил в номинации «Лучшая песня». В своей речи, которую в прямом эфире транслировала NBC, исполнитель сказал: «Это просто... просто fucking блеск!»

Комиссия постановила, что это замечание было «явным оскорблением современных общественных норм для широковещательных средств

---

1 *www.cnn.com/2006 года./POLITICS/07/17/bush.tape/index.html*

2 Джефф Джарвис (Jeff Jarvis) «America gives a shit» (Америка как источник shit»), *Reason Magazine*, октябрь 2006 года, *www.reason.com/news/show/36821.html*.

массовой информации»[1], и предупредила, что будет штрафовать и даже отбирать лицензии у станций, передающих подобные «перлы».[2]

В 2006 году перечень запрещенных слов был расширен. Актриса и певица Николь Ричи как-то поделилась с фотомоделью Пэрис Хилтон возмущением по поводу реалити-шоу, в котором Ричи пришлось работать на ферме: «Почему они называют это „Простой жизнью“? Ты когда-нибудь пыталась вытащить коровье shit из сумочки Прада? Это fucking нелегко».[3] Постановление FCC об использовании метафоры экскрементов в данном случае могло означать, что выражения президента Буша в глазах сотрудников комиссии являлись «допустимо вульгарными».

Федеральный суд обратил политику комиссии против таких «слов-паразитов», применявшихся десятки лет.[4] Конгресс быстро принял закон о восстановлении строгих стандартов FCC, и дело было передано в Верховный суд весной 2008 года.[5] Новый стандарт был принят после того, как изучили статистику, показывающую, насколько чаще в фире стали употребляться бранные слова: в 2000 году – менее 50 раз, в 2004 году – 1,4 миллиона. Конгресс мог считать, что новый закон о свободе слова отражает мнение общества.

В соответствии с Первой поправкой правительство, как правило, не ограничивает свободу слова. Власти не могут редактировать газеты, даже чтобы расширить объем информации, доносимой до читателей. Верховный суд отменил закон штата Флорида о «праве на ответ» кандидатов в выборные органы власти газетным атакам, так как посчитал закон противоречащим Конституции.[6]

Несмотря на это, в 2006 году некое федеральное агентство попыталось убрать часть информации из эфира, используя правила, которые «предположительно» относились даже к откровенному диалогу двух лидеров свободного мира. Десятки газет полностью напечатали слова президента Буша; любой пользователь Интернета мог прослушать

---

1 Странный стандарт, сам по себе, поскольку вещательное собщество может слышать и видеть только то, что позволяют правила комиссии.

2 *www.fcc.gov/eb/Orders/2004 года./FCC-04-43A1.html*

3 *www.fcc.gov/omnibus_remand/FCC-06-166.pdf*

4 Дело «Fox Television Stations и др. против FCC», апелляционный суд, Docket Nos. 06-1760-ag (L), 06-2750-ag (CON), 06-5358-ag (CON), 4 июня 2007 года.

5 Protecting Children from Indecent Programming Act (Акт о защите детей от приучения к непристойностям), предложенный сенатором Джоном Рокфеллером (John Rockefeller) мог бы перевернуть решение суда по делу «Fox Television Stations и др. против FCC», *pressesc.com/01184929170_senate_indecency_bill*; Линда Гринхаус (Linda Greenhouse) «Justices take up on-air vulgarity again» (Судьи снова разбираются с непристойностями в эфире), *New Your Times* от 18 марта 2008 года.

6 Дело «Miami Herald Publishing Company против Торнильо», Верховный суд США, 418 U. S. 241 (1974).

аудиозапись. Несмотря на жалобы в FCC о неприличном содержимом в эфире, американцы обычно сопротивляются попыткам правительства «нянчить» телепередачи.[1]

Как регулируется эфир

Комиссия FCC сохраняла контроль над содержанием эфира, пока средств передачи данных в эфире было достаточно мало. По общему мнению, доступные частоты были дефицитом, а правительство должно было следить за тем, чтобы диапазоны использовались в интересах общества. Как пояснил Верховный суд в 1978 году, средства массового вещания проникли «исключительно глубоко в жизнь всех граждан Америки», поэтому правительство особым образом заинтересовано в защите общественной аудитории от нежелательного содержимого теле- и радиопередач.[2]

Революционные изменения в технологиях связи обесценили обе причины. В цифровую эпоху у битов гораздо больше способов добраться до пользователей, так что телевидение и радио перестали быть исключительно важными источниками информации. С минимальными затратами кто угодно может, сидя дома или в закусочной Starbucks, выбрать нужное из миллиардов веб-страниц или десятков миллионов блогов. Эксцентричный теле- и радиоведущий Говард Стерн перебрался с общественного радио на спутниковое – там слова никто не контролирует. Более 90% американских телезрителей получают сигнал вещания не с телевышки на комнатную или внешнюю антенну, а по кабелю или со спутника. RSS-трансляции предоставляют новости миллионам пользователей мобильных устройств. В наши дни радиостанции и телевышки больше не являются ни желанными, ни особо влиятельными источниками информации.

В цифровую эпоху у битов гораздо больше способов добраться до пользователей, так что телевидение и радио перестали быть исключительно важными источниками информации.

Если государство желает защитить детей от всех возможных источников негативной информации, то ему необходимо постоянно расширять и совершенствовать законодательную базу. К слову говоря, дело идет именно к тому – ведется работа по расширению полномочий FCC на спутниковое и кабельное телевидение.[3]

---

1 *www.televisionwatch.org/junepollresults.pdf*

2 Заключения судьи Стивенса по делу «FCC против Pacifica Foundation и др.», 438 U.S. 726, 748.

3 Family and Consumer Choice Act (Акт семейного и потребительского выбора) 2007 года совместно продвинут членами Палаты представителей Дэниелом Липински и Джеффом Фортенберри.

Выживание с помощью средств беспроводной связи

Поразительный пример повсеместного распространения беспроводных сетей связи, несмотря на ограничения частотных диапазонов, был явлен после разрушения Всемирного торгового центра 11 сентября 2001 года. В Нижнем Манхэттене (район Нью-Йорка) несколько дней связь поддерживалась только средствами беспроводной коммуникации.[1] Нечто похожее имело место после того, как в декабре 2006 года в юго-восточной Азии проложенные по дну океана кабели связи были повреждены землетрясением.

Революция в средствах связи, однако, предоставляет и другие варианты. Если кто угодно может разместить информацию, доступную неограниченному числу людей, то интересы государства по ограничению вещания должны снизиться, а не вырасти. Если нет дефицита, возможно, государству следует отказаться от возможности контролировать все радио- и телепередачи, как в свое время оно отказалось от контроля периодических изданий. В этом случае вместо расширения соответствующих полномочий FCC необходимо снизить их или даже снять полностью, так же как Верховный суд отменил закон штата Флорида о газетной цензуре.

Участники рынка, у которых уже есть доля в эфире, заявляют, что диапазон – доступные частоты радиоволн – должен оставаться ограниченным и контролируемым государством ресурсом. Диапазон частот «не резиновый» и должен использоваться в интересах общества.

Но оглянитесь. Да, есть несколько станций диапазонов СВ (AM) и УКВ (FM). Но вокруг вас в эфире ежеминутно проходят тысячи, возможно, десятки тысяч сеансов радиосвязи. Большинство американцев постоянно носят с собой двусторонние радиостанции – те штуки, которые мы чаще называем сотовыми телефонами, – и большинство подростков общается с их помощью почти непрерывно. Радиоприемники и телевизоры могли бы быть более изощренными устройствами и использовать среду связи лучше, чем сотовые телефоны.

Заявление о том, что частотный диапазон является дефицитным ресурсом, как научно обоснованный аргумент не выдерживает критики. Эту точку зрения всеми силами поддерживает не желающая делиться своим пирогом медиаиндустрия. Владельцы лицензий – существующие вещательные станции и сети – имеют резон обезопасить свои ниши в диапазоне от любого реального или воображаемого риска искажения сигнала. Проталкивая запреты на технологические новшества,

[1] Питер Мейерс (Peter Meyers) «In crisis zone, a wireless patch» (Беспроводной участок в кризисной зоне), *New York Times* от 4 октября 2001 года.

руководители индустрии могут ограничивать конкуренцию, избегая капиталовложений. Две стороны медали – заинтересованность государства в поддержании искусственного дефицита рабочих диапазонов ради правового регулирования свободы слова и заинтересованность руководства медиаиндустрии в поддержании дефицита ради снижения конкуренции и издержек в настоящее время сильно ограничивают культурную и техническую активность, принося вред обществу.

Чтобы понять, какие объединенные силы создали современный мир цензуры радио и телевидения, нужно проследить историю изобретения технологии беспроводной связи.

От беспроводного телеграфа к беспроводному хаосу

Красный, оранжевый, желтый, зеленый, синий – цвета радуги – одновременно различаются и представляют собой однородные явления. Любой ребенок, познакомившись с набором красок, знает, что все цвета разные. При этом все цвета однородны, потому что представляют собой воспринятое глазом электромагнитное излучение. Световое излучение распространяется в виде волн с очень высокой частотой колебания. Единственное различие между красным и синим цветами с точки зрения физики – то, что волна красного цвета имеет частоту колебаний примерно 450 триллионов раз в секунду, а волна синего – примерно на 50% больше.

Так как спектр видимого цвета непрерывен, между красным и синим цветами есть бесчисленное множество цветов. Смешение световых волн с разными частотами дает другие цвета, например смешение в равной доле синего и красного порождает оттенок розового – пурпурный.

В 1860-х британский физик Джеймс Кларк Максвелл открыл, что свет является разновидностью электромагнитных волн. Из полученных формул следовало, что могут существовать и другие волны, не воспринимаемые глазом человека. Более того, эти волны окружают нас с самого начала времен. Солнце и звезды испускают излучения; электромагнитные волны появляются при вспышке молнии. Никто не подозревал об их существовании, пока уравнения Джеймса Максвелла не показали, что это возможно. Есть очень много невидимых волн различных частот, путешествующих со скоростью света.

Эра радиоволн началась в 1887 году с демонстрации опыта немецкого физика Генриха Герца. Физик приблизил друг к другу два конца провода, оставив между ними небольшой зазор. Когда в нескольких метрах был инициирован мощный электрический разряд, между концами провода проскочила искра. Инициирующий разряд создал электромагнитное излучение, которое вызвало электрический ток в незамкнутом кольце из провода. Искра замкнула электрическую цепь. Генрих Герц создал первую в мире антенну и получил радиоволны, которые она уловила. В честь физика названа единица измерения частоты: один герц

(сокращенно Гц) – это один период колебания в секунду. Килогерц (кГц) означает тысячу колебаний в секунду, мегагерц (мГц) – миллион колебаний. В частотных диапазонах СВ (AM) и УКВ (FM) находятся величины, измеряемые в кило- и мегагерцах.

Гульельмо Маркони не был ни математиком, ни ученым. Он был изобретателем-самоучкой. Когда Генрих Герц демонстрировал свой эксперимент, Гульельмо Маркони было всего 13 лет. За следующие десять лет юноша методом проб и ошибок разработал более эффективные способы генерирования и приема радиосигналов на больших расстояниях.

В 1901 году изобретатель, находясь в британской колонии Ньюфаундленд, получил один символ кода Морзе из Англии. На волне успеха «Компания беспроводного телеграфа Маркони» вскоре начала оснащать корабли устройствами связи друг с другом и с землей. Когда «Титаник» отправился в свое трагическое путешествие, на борту было установлено оборудование производства «Компании беспроводного телеграфа Маркони». Основной работой операторов на борту была передача персональных сообщений пассажиров, но лайнер также получил не менее двух десятков предупреждений от других кораблей о возможности столкновения с айсбергами.[1]

Слова «беспроводной телеграф» в названии компании указывают на самое главное ограничение первых радиосистем. Технология была задумана как средство связи между двумя удаленными объектами. Радио решило главную проблему телеграфа. Катастрофа, саботаж, война не могли прервать передачу, так как не было никаких информационных кабелей. Но был и принципиальный недостаток: радиограмму мог прочитать кто угодно. Поразительная возможность одновременной передачи информации одновременно тысячам людей первоначально рассматривалась, как недостаток. Кто станет платить за передачу беспроводного телеграфного сообщения, которое может услышать кто-то еще?[2]

Количество пользователей радиосвязи росло, и появилась другая проблема, которая и сегодня ограничивает прогресс радио и телевидения. Если несколько близко расположенных станций одновременно ведут передачу, то их сигналы накладываются друг на друга. Крушение «Титаника» показывает пример возможного эффекта одновременной передачи. На следующее утро после столкновения с айсбергом американские газеты уверенно сообщили, что все пассажиры спаслись, а лайнер отбуксирован к берегу.

Ошибка возникла в результате получения радистом пары совмещенных сообщений-морзянок. Одно судно отправило в эфир вопрос «Все ли пассажиры «Титаника» спасены?», а другое, в это же время, – от-

---

1 *www.titanic-titanic.com/warnings.shtml*

2 Термин «радио» стал общепринятым только после Второй мировой войны.

чет о своих действиях: «300 миль западнее Титаника буксируем танкер в Галифакс».[1] На кораблях было оборудование и радисты. Но не было никаких правил относительно того, как и когда пользоваться радиосвязью.

Люди, использовавшие первые передатчики Маркони, часто ошибались, потому что не имели возможности «подстроить» частоту. При всем своем уме, позволившем существенно увеличить дальность связи, изобретатель применял все тот же способ Генриха Герца – генерацию мощных разрядов. Разряды создавали электромагнитные волны в радиодиапазоне. Можно было настраивать количество энергии и длительность разряда (для получения «точек» и «тире» кодов Морзе), но и только. Сигнал от одного радиста был подобен сигналу от другого. При одновременной передаче начинался хаос.

Множество цветов видимой части спектра, сливаясь, дают белый свет. Цветной фильтр пропускает только определенную часть волн видимого цвета, задерживая остальные. Если вы посмотрите сквозь красный фильтр, то весь мир предстанет перед вами в виде более светлых или более темных оттенков красного. Радиосвязь нуждалась в чем-то подобном для спектра радиочастот. Нужен был способ для создания радиоволн на одной частототе или хотя бы в узком диапазоне, чтобы приемник сигнала мог выделить нужную волну и отделить остальные. К счастью, такая технология уже существовала.

В 1907 году Ли Де Форест запатентовал технологию, сделавшую возможной создание «Компании радиотелефонии Де Фореста». Работа компании заключалась в передаче голоса и даже музыки по радиоволнам. Когда компания 13 января 1910 года осуществила широковещательную передачу выступления Энрико Карузо в театре Метрополитен Опера, голос певца достиг кораблей в море. Любители музыки толпились у приемников в штатах Нью-Йорк и Нью-Джерси. Эффект был порясающим. В последующие несколько лет сотни радиолюбителей включились в действо. Они транслировали музыку, какую только могли заполучить, всем, кто желал слушать.

До тех пор пока не существовало соглашений о частотных диапазонах, радиосвязь оставалась чем-то вроде стрельбы с завязанными глазами по движущейся мишени.

Но до тех пор пока не существовало соглашений о частотных диапазонах, радиосвязь оставалась чем-то вроде стрельбы с завязанными глазами по движущейся мишени. То, что газета «New York Times» назвала «бездомными песенными волнами»: когда на трансляцию выступления Энрико Карузо накладывалось вещание другой станции, которая, «несмотря на все мольбы», упорно работала на той же частоте в 350 кГц. Кому-то повезло

[1] Карл Баарслаг (Karl Baarslag) «S O S to the Rescue» (С О С для спасения), Oxford University Press, 1935, 72.

«словить кайф» от голоса певца, а кто-то мог получить только нудный код Морзе: «Я только что взял пива».[1]

Радиоволны на выделенных каналах

Формирующаяся радиопромышленность не могла развиваться в таких условиях. Коммерческие интересы поддержали заявления со стороны военно-морского флота о том, что любительские сигналы мешают морской связи. Крушение «Титаника», при том что оно мало зависело от помех в радиосвязи, подстегнуло действия правительства. 12 мая 1912 года Уильям Олден Смит обратился к Сенату США с просьбой выработать правила использования радиосвязи. «Когда весь мир оплакивает общую потерю... – заявил сенатор Смит, – неужели не пора очистить море от конфликтующих диалектов и начать мудро управлять этим новым слугой человечества?»[2]

Высокие частоты

С годами технологические достижения делали возможным использование радиоволн со все более высокими частотами. В начале развития телевидение вещало на «сверхвысоких частотах» (Very High Frequencies, VHF). Частота таких волн превышала частоты коротковолнового радио. Спустя некоторое время станции начали занимать «ультравысокие частоты» (Ultra High Frequencies, UHF). В настоящее время порогом коммерческого диапазона является частота несущего сигнала 77 ГГц (77 000 МГц). В общем случае, высокочастотный сигнал затухает с увеличением расстояния быстрее, чем низкочастотный. Поэтому высокочастотное вещание обычно ограничивается конкретной местностью или городом. Все радиоволны движутся с одной и той же скоростью – скоростью света, – и чем выше частота, тем меньше длина волны.

Акт о радио 1912 года (Radio Act) ограничил публичное радиовещание, сделав его привилегией только владельцев лицензий. Лицензии «выдавались министром торговли и трудовых отношений после рассмотрения заявления». Выдавая лицензию, министр ограничивает некоторый диапазон «только для использования указанной станцией с целью предотвращения интерференции сигналов и только теми часами, в течение которых указанная станция вправе осуществлять вещание». Акт зарезервировал для нужд государства диапазон от 200 до

---

[1] «Wireless melody jarred» (Беспроводная музыка из коробки), *New York Times* от 14 января 1910, 2.

[2] *www.titanicinquiry.org/USInq/USReport/AmInqRepSmith01.php*

500 кГц, в котором возможна наиболее качественная связь на дальние расстояния. «Коротковолновой диапазон» частот выше 1500 кГц посчитали бесполезным из-за технических ограничений и предоставили в распоряжение радиолюбителей. Частота в 1 МГц была зарезервирована для сообщений о бедствиях. Специальные станции прослушивают эту частоту каждые 15 минут. (Сто лет назад это могло бы спасти пассажиров и экипаж «Титаника». Радисты близкого к «Титанику» корабля в нужное время отдыхали и пропустили сигналы бедствия.) Оставшийся диапазон министр мог назначать коммерческим радиостанциям и частному бизнесу. Рассматривая радио как «беспроводную телеграфию», Акт о радио объявил правонарушением прослушивание радиосигнала тем, кому сигнал не предназначался.

Многое изменилось с 1912 года. Способы применения радиоволн стали более разнообразными, изменились границы частотных диапазонов, да и спектр доступных технике частот значительно расширился. Используемое в настоящее время деление спектра частот в графическом изображении похоже на разноцветную мозаику. Это результат десятков «соломоновых решений» FCC (рис. 8.1). Государство все еще ведет контроль и учет использования различных диапазонов. Цель этого – предотвратить взаимное наложение сигналов радиолюбителей и (или) правительственной связи. Частное вещание должно происходить с ограниченной мощностью и только в пределах разрешенного диапазона. Когда радиостанций было немного, оговоренную Актом о радио процедуру их лицензирования удавалось соблюдать без проблем. Любителям поболтать в эфире предоставили свою «территорию», так же как военным и коммерческим станциям.

Всего за десять лет положение круто изменилось. 2 ноября 1920 года радиостанция в Детройте освещала избрание Уоррена Хардинга президентом США, транслируя информацию, получаемую по телеграфу. Радио больше не было способом связи «один-на-один». Год спустя станция в Нью-Йорке транслировала финальный бейсбольный матч между командами «Giants» и «Yankees», подачу за подачей. Трансляция спортивных новостей родилась в тот день, когда оператор радиостанции начал повторять в эфире сообщения, получаемые по телефону от репортера на стадионе.[1]

Общество все больше осознавало возможности радиосвязи. Первые лицензии на вещание в 1921 году получили пять станций.[2] Год спустя по лицензии вещали уже 670 станций. Количество радиоприемников за год выросло с 50 000 до 600 000 и больше, возможно, даже до миллиона.[3] Станции, вещающие на одной частоте в одной местности, делили

---

[1] Эрик Барноу (Erik Barnouw «A Tower in Babel» (Вавилонская башня), Oxford University Press, 1966 год, 69, 85.

[2] Там же, 91, 104.

[3] «Asks radio experts to chart the ether» (Радиоэксперты составляют карту эфира), *New York Times* от 28 февраля 1922 года, 16.

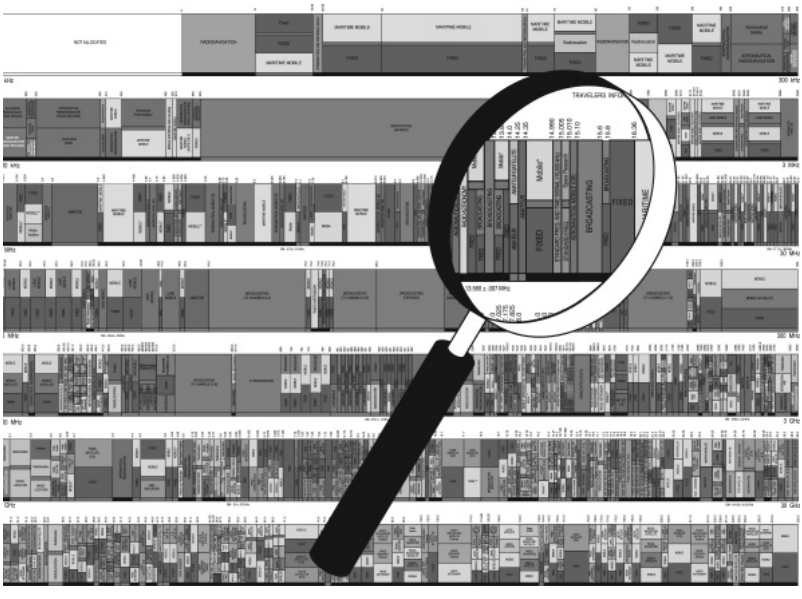


Рис. 8.1. *Деление диапазона частот в США. Границы диапазона – от 3 кГц до 300 ГГц. Диапазон начинается в верхнем левом углу и заканчивается в нижнем правом. Шкала диапазонов – логарифмическая, то есть каждый последующий ряд имеет плотность делений в 10 раз выше предыдущего. К примеру, верхний блок во втором ряду – это диапазон СВ (AM), примерно 1 МГц. В нижнем ряду тот же диапазон частот имеет ширину около 0,0005 мм*

Источник: www.ntia.doc.gov/osmhome/allochrt.pdf

между собой эфирное время. Когда радиовещание стало выгодным делом, рост замедлился.

12 ноября 1921 года истек срок лицензии станции компании «Intercity Radio Co» на вещание в Нью-Йорке. Герберт Гувер, министр торговли, отказался продлить лицензию на том основании, что для станции нет свободной частоты. Компания подала иск в суд и выиграла.[1] Суд постановил, что министр имел возможность выбрать частоту, но не имел полномочий отказать в продлении лицензии. После вступления в силу Акта о радио в 1912 году система лицензирования частот стала «в сущности тем же самым, что и система разрешений для 25 000 торговых кораблей». Суть замечания в том, что министр должен регулировать действия радиостанций подобно движению торговых кораблей в океане. Можно указать свободные трассы, но нельзя отказать в возможности плавать.

[1] Дело «Гувер против Intercity Radio», № 3766, апелляционный суд округа Колумбия, 52 App. D. C. 339, 5 февраля 1923 года.

Перед радиоиндустрией остро встал вопрос о наведении порядка. С целью выработать новые соглашения, пока не начался настоящий хаос, министр Гувер в 1922 году организовал Национальную конференцию по вопросам радиосвязи. Объясняя причины своих действий, министр заявил, что диапазон радиочастот является «великим национальным достоянием» и что «в интересах общества чрезвычайно важно установить, кто будет осуществлять вещание, в каких условиях и какую информацию передавать... Огромное число подписчиков нуждается в защите от шумов, которые могут появиться в их устройствах». Эфир, добавил министр, нуждается в «полиции», которая будет отслеживать «хулиганов, создающих помехи вещанию».[1]

По инициативе министерства частотный диапазон от 550 кГц до 1350 кГц был поделен на «каналы» шириной 10 кГц, чтобы вместить больше станций. В названии «каналы» заметно влияние морской терминологии. У границ каждого диапазона оставлены свободные частоты, потому что широковещательные сигналы неизбежно расширяются, сокращая тем самым рабочий диапазон. Путем взаимных соглашений министерству удалось решить проблему распределения частот. Владельцы радиостанций оценили удобство предложенных министром мер. Новичкам бизнеса, наоборот, пришлось туговато. Так, одной религиозной группе, объявлявшей о скором приходе конца света, отказали в выделении свободного диапазона, предложив закупать эфирное время у имеющихся станций. В конце концов, это сэкономило верующим средства: полгода спустя, когда «конец света» наступил, собственная станция была уже не нужна.[2] Система Гувера встретила и одобрение Конгресса – она просто работала, без дополнительных законов.

Однако с увеличением числа диапазонов выросло и количество связанных с этим проблем. В 1924 году станции WLW и WMH спокойно вещали в Цинциннати на одной частоте, до тех пор пока министерство не «посадило» на два диапазона три станции. Долго это не могло продолжаться. В 1925 году корпорация Zenith Radio получила лицензию на вещание на частоте 930 кГц в Чикаго, но только в среду с 22 часов до полуночи, и только если в это время не вещает станция из Денвера. Не спрашивая разрешения, станция Zenith начала вещание на частоте 910 кГц. Эта частота была свободна, так как по договору была предоставлена Канаде. Министр наложил на корпорацию Zenith Radio штраф. Корпорация (успешно) оспорила полномочия министра в суде.[3] Головной боли министру прибавили письма от генерального проку-

[1] Герберт Гувер, выступление на первой Национальной конференции по радиосвязи 27 февраля 1922 года, мемуары Г. Гувера, т. 2 «The Cabinet and Presidency», MacMillan, 1952, 140.

[2] Воспоминания Герберта Кларка Гувера, проект исследования устной истории, ветка «Радио», Колумбийский университет, январь 1951 года, 12.

[3] Дело «Соединенные Штаты против Zenith Radio Corporation и др.», суд Северного округа штата Иллинойс, 12 F.2d 614; 16 апреля 1926 года.

ора: Акт о радио, разработанный еще до того, как публичное радиовещание не существовало даже в проектах, был составлен настолько неясным стилем, что, возможно, не предоставлял министру торговли и трудовых отношений права регулировать ни частоту, ни мощность сигнала, ни время вещания, ни что бы то ни было.

Министру оставалось только развести руками. Любой мог установить передатчик и выбрать частоту – на рассмотрении в это время находилось 600 заявлений – но «на свой страх и риск». Результатом неконтролируемого вещания стал предсказанный министром «хаос в эфире».[1] Ситуация была намного хуже, чем в 1912 году, поскольку имелось множество мощных передатчиков. Станции создавались, метались по диапазону в поисках свободной частоты и повышали мощность сигнала, чтобы заглушить сигналы от таких же станций. Радио стало бесполезным, особенно в крупных городах. Конгрессу пришлось начать действовать.[2]

Национализация полосы частот

Положения Акта о радио 1927 года все еще действительны. Они определяют полосу радиочастот как исчерпаемый национальный ресурс, использование которого регулируется государством.

Положения Акта о радио 1927 года все еще действительны. Они определяют полосу радиочастот как исчерпаемый национальный ресурс, использование которого регулируется государством.

Цель принятия Акта – установить государственный контроль для всех каналов «радиопередач; а также предоставить возможность использования этих каналов, но не на праве собственности, гражданами, фирмами или корпорациями на ограниченные периоды времени в соответствии с лицензиями, выдаваемыми от имени федерального правительства…» Общество может использовать полосу частот в соответствии с установленными правительством условиями, но не может полностью или частично владеть ею. Вопросы лицензирования перешли к новому органу власти – Федеральной комиссии по радиосвязи (Federal Radio Commission, FRC). У общественности были основания ожидать удовлетворения запросов на выдачу лицензий: «Орган власти, занимающийся вопросами лицензирования, в соответствии с общественным удобством, интересами или необходимостью… выдает претенденту надлежащую лицензию на станцию…» Акт о радио предусматривал ситуацию, когда количество заявлений о предоставлении лицензии превышает емкость полосы

[1] «Hoover asks help to avoid air chaos» (Гувер просит о помощи, чтобы справиться с хаосом), *New York Times* от 10 июля 1926 года.

[2] Дэниел Клейн (Daniel Klein) в «Rinkonomics» замечает, что там, где интересы совпадают, можно обойтись без регулирования, *www.econlib.org/library/Columns/y2006/Kleinorder.html*.

радиочастот. В случае наличия конкуренции между претендентами «орган должен установить такое распределение лицензий, диапазонов..., периодов времени действия и мощности в разных штатах и сообществах, чтобы создать справедливое, эффективное и равноправное для всех обслуживание».[1]

Слова о «соответствии с общественным удобством, интересами или необходимостью» – эхо выступления министра Гувера в 1922 году о том, что диапазон радиочастот является «великим национальным достоянием» и об «интересах общества». Неслучайно Акт был разработан на пике скандала в администрации Белого дома по поводу предвзятой процедуры передачи в разработку нефтяного месторождения «Teapot Dome» (Крышка чайника). Месторождение располагалось на территории штата Вайоминг. Компания Sinclair Oil получила в 1923 году права на ее разработку, подкупив министра внутренних дел. Несколько лет следствие по преступлению велось на уровне Конгресса и Федерального суда. Министр был приговорен к тюремному заключению. К началу 1927 года добропорядочное использование национальных ресурсов в интересах общества стало главным интересом внутренней политики.

В соответствии с Актом о радио 1927 года диапазон радиочастот стал чем-то вроде федеральной территории. Международные соглашения требовали исключить наложение сигналов сопредельных государств. Но в пределах территории США федеральное правительство решало, кто имеет право осуществлять вещание на частоте, а иногда даже определяло, какую информацию можно, а какую нельзя выпускать в эфир – в точности, как требовал министр Гувер пять лет назад.

Эволюция комиссии по радиосвязи

В 1934 году название «Федеральная комиссия по радиосвязи» было изменено на «Федеральная комиссия по коммуникациям» (FCC), поскольку на комиссию были также возложены функций контроля телефонных и телеграфных коммуникаций. Когда телевидению потребовался свой частотный диапазон, влияние FCC стало распространяться и на телевизионное вещание.

Козлиные тестикулы и Первая поправка

Акт о радио 1927 года постановил, что FRC не может ограничивать свободу слова в эфире. «Никакая часть акта не подразумевает и не может быть истолкована таким образом, что орган, занимающийся вопросами

[1] Акт о радио 1927 года, документ № 632, 23 февраля 1927 года, 1, 9.

PREACHES FUNDAMENTALISM PRACTICES GOAT-GLAND SCIENCE

How a Famous Surgeon Combines Old-Time Religion and New-Fangled Operations on a Strange Medico-Gospel Farm

Рис. 8.2. *Статья о клинике «доктора» Бринкли, специализурующейся на пересадке козлиных тестикул. Сам «доктор» показан слева, на руках у него ребенок («по имени Билли»), родившийся, как сказано в статье, «после успешной пересадки тестикул»*

Журнал «New York Evening» от 11 сентября 1926 года. Микрофотокопия предоставлена Библиотекой Конгресса США

лицензирования, может устанавливать цензуру… и никакое правило или ограничение… не может как-либо ограничивать право на свободу слова, реализуемое с помощью средств радиосвязи».[1] При случае неизбежно проявлялось внутреннее противоречие: с одной стороны, **FRC** должна при выдаче или продлении лицензий соблюдать общественные интересы и нормы; с другой стороны, она не может вводить цензуру. Характерный пример – дело о выдаче лицензии радиостанции **KFKB** из штата Канзас. Владельцем станции был Джон Ромул Бринкли, «козлиный хирург» (рис. 8.2). Гнев, который в 2004 году обрушился на CBS, показавшую на миг грудь Джанет Джексон, – то, из-за чего многие телестанции боялись транслировать фильм «Спасти рядового Райана» на День ветеранов, и пресловутая реплика президента Буша

[1] Акт о радио 1927 года, 29.

Тони Блэру – все это последствия действий FCC против рядового американского афериста.

Джон Бринкли родился в 1885 году. Купив диплом в Университете гомеопатических методов лечения (Канзас-Сити), он стал «доктором» с правом медицинской практики в штате Канзас. Одно время работал санитаром на мясокомбинате «Swift & Co». В 1917 году открыл частную практику в небольшом городке Милфорд, расположенном примерно в 70 милях к западу от Топики. Один из пациентов пожаловался на снижение потенции, назвав свое состояние «спущенной камерой». Вспомнив работу на скотобойне, Бринкли сказал: «Проблема исчезнет, если пересадить вам пару козлиных тестикул». «Так почему бы вам не сделать это?» – ответил пациент. Дальняя комната была превращена в операционную, и дело пошло. Бринкли стал проводить 50 трансплантаций в месяц, по 750 долларов за каждую. Вскоре он заметил, что клиентов больше привлекает увеличение сексуальной активности, чем восстановление детородной способности.[1]

Бринкли, в юности поработавший в телеграфной конторе, понимал потенциал технологий связи. В 1923 году он открыл первую в Канзасе радиостанцию под названием KFKB («Kansas First, Kansas Best» – «Первая в Канзасе, лучшая в Канзасе»). Название станции можно было также расшифровать как «Kansas Folks Know Best» («Канзасцы знают, что лучше»). Передавали, в основном, музыку в стиле кантри, пламенные проповеди и медицинские советы от доктора Бринкли. Слушатели могли сообщать о своих недомоганиях, так что обычно советы доктора сводились к предложению заказать по почте какое-нибудь патентованное средство (изобретенное, конечно же, самим доктором Бринкли). Типичное начало передачи: «У нас письмо от Тилли. Она сообщает, что десять лет назад перенесла операцию, и жалуется на здоровье. Я считаю, что в операции не было наобходимости, и едва ли стоит ожидать, что после удаления яичников детородная функция будет работать нормально. Советую принимать «Женский тоник» № 50, 67 и 61. Через три месяца регулярного приема этот комплекс даст вам желаемый результат (если лекарства вообще могут здесь помочь)».[2]

Станция KFKB была оборудована чрезвычайно мощным передатчиком. Его сигнал можно было поймать даже в центре Атлантики. По результатам национального опроса, станция KFKB оказалась в Америке самой популярной, получив в четыре раза больше голосов, чем ближайший конкурент. Джон Бринкли получал по три тысячи писем в день (невероятный успех). Бывало, клиника в Милфорде принимала

---

[1] Барноу, 169ff; Джеральд Карсон (Gerald Carson) «The Roguish World of Dr. Brinkley» (Жульнический мир доктора Бринкли), Rinehart and Co., 1960, 33ff. Новая биография доктора Бринкли: Поуп Брок (Pope Brock) «Charlatan» (Шарлатан), Crown, 2008.

[2] Дело «KFKB Broadcasting Assn против FRC», 60 App. D. C. 79, 47 F.2d 670, 2 февраля 1931 года.

до пятисот пациентов в день. Однако Американская медицинская ассоциация (American Medical Association) – по наводке конкурирующей радиостанции – расценила действия доктора Бринкли как шарлатанство. FRC в свою очередь решила, что своевременное продление лицензии на вещание станции KFKB не находится «в соответствии с общественным удобством, интересами или необходимостью». Джон Бринкли возразил, что отказ в продлении лицензии – не что иное, как цензура и ограничение свободы слова.

Апелляционный суд своим знаменательным решением принял сторону FRC. Согласно мнению суда цензура была первичным средством сдерживания, но не имела места в деле Джона Бринкли; комиссия «всего лишь воспользовалась своим несомненным правом высказать свое мнение относительно прежнего поведения апеллирующей стороны». Главным аргументом послужили слова американского государственного деятеля Альберта Галлатина, сказанные более двухсот лет назад о первичных средствах сдерживания прессы: «Нелепо заявлять, будто наказание за некоторое действие не ограничивает свободу выполнять это действие».[1]

Для обоснования действий FRC суд использовал метафору земель общественного пользования: «Поскольку число доступных для радиовещания частот ограничено, комиссия вынуждена принимать решение о сущности и качестве сервиса, подлежащего регистрации... Очевидно, что в частотном диапазоне нет места для каждой компании или философского направления».

«Вынуждена» и «очевидно». Всегда трудно опровергнуть аргументы, истинность которых объявлена само собой разумеющейся. Судья Феликс Франкфуртер в 1943 году сформулировал принцип, который часто цитировался: «Тяжелое положение, в котором находилась радиосвязь до 1927 года, имело причиной некоторые базовые факты относительно радиосвязи как средства коммуникации: возможности радио ограничены, они недоступны для всех, кто желал бы ими воспользоваться, диапазон радиочастот не может вместить всех желающих. Существует очевидное физическое ограничение числа станций, которые могут вещать без взаимного наложения сигналов».[2]

Таковы были ограничения технологии того времени. Это было истиной, но лишь в рамках уровня развития техники. Реалии середины

---

[1] Цитируется Энтони Льюисом (Anthony Lewis) в книге «Make No Law» (Обойдемся без закона), Vintage, 1991, с. 60. Энтони Льюис цитирует книгу Леви (Levy) «Emergence of a Free Press» (Крайности свободной прессы), с. 302–303).

[2] Дело «National Broadcasting Co. против Соединенных Штатов и др.», Верховный Суд США, № 554, 319 U.S. 190; 63 S. Ct. 997; 87 L. Ed. 1344; 1943 U.S. LEXIS 1119; 1 Media L. Rep. 1965; 10 и 11 февраля 1943 года, обжаловано; 10 мая 1943 года, принято решение. В отрывке цитируются два учебника по радиосвязи, опубликованные в 1933 и 1937 годах.

прошлого века никогда не были универсальными физическими законами и больше не являются ограничениями технологии. Инженерные решения последних двух десятилетий практически сняли «физическое ограничение» на количество возможных станций в эфире. Аргумент неизбежности исчерпания радиодиапазона больше не поможет государству оправдывать запрет использования радиоволн.

Обширная система контроля, обеспечивающая эффективное использование ограниченной радиосвязи в те времена, довольно медленно адаптировалась к новым реалиям. Бюрократия, как всегда, отстает от технологического прогресса. FCC пытается централизованно и своевременно удовлетворять потребность в ресурсах. Но технология может внезапно вызвать изменение инфраструктуры, а силы, правящие рынком, могут внезапно вызвать изменение спроса. Централизованное планирование в FCC работало не лучше, чем в Советском Союзе.[1]

Более того, многие силы, получающие прибыль от старых технологий, будут счастливы видеть старые правила неизменными. Подобно удачливым арендаторам общественных угодий отдельные владельцы лицензий на вещание совершенно не заинтересованы в конкурентах по использованию их владений. Чем больше поставлено на карту, тем разнообразнее средства воздействия на бизнес. Лицензии на радиовещание имели ценность почти с самого начала эпохи радио, и с ростом числа желающих быть услышанным в эфире ценность лицензий увеличивается. В 1925 году в Чикаго лицензия стоила 50 000 долларов. С развитием рекламы и объединением станций в сети цена возросла до семизначной. После вступления в силу Акта о радио 1927 года споры между станциями подлежали рассмотрению в судебном порядке, с пересылкой в Вашингтон и борьбой дружественных преставителей в самом Конгрессе. Все это было доступно только для станций с большими средствами. Поначалу было много университетских станций, однако с увеличением стоимости эфирного места FRC постепенно стала их вытеснять. В итоге многие образовательные радиостанции были проданы коммерческим вещателям. *Фактическое* положение радиосвязи хорошо описывается словами одного историка: «На словах защищая интересы общества,... на деле комиссия выбирает, как лучше угодить интересам коммерческих радиостанций».[2]

Переход к отказу от регулирования диапазона

Нажимая кнопку на брелоке, чтобы открыть дверцу автомобиля, вы передаете радиосигнал. Этот сигнал тоже занимает какую-то часть ра-

---

[1] Аналогия принадлежит Майклу Маркусу.

[2] Пендлтон Херринг (Pendleton Herring) «Politics and radio regulation» (Политика и регулирование радиосвязи), «Harvard Business Review», январь 1935.

диодиапазона. Для брелока – вашей радиостанции – действительны те же законы физики, что и для бостонской станции WBZ, непрерывно вещающей с тех пор, как в 1921 году она стала первой коммерческой радиостанцией на востоке США. Но здесь есть два важных отличия. Во-первых, сотни миллионов брелоков ежедневно включают и отключают автосигнализацию. Во-вторых, мощность передатчика станции WBZ составляет 50 киловатт, а мощность брелока – меньше 0,0002 ватта.

Если бы правительство все еще лицензировало каждый радиопередатчик – как постановил Конгресс после радиохаоса 1920-х, – то ни радиоуправление автосигнализацией, ни другие широко распространенные средства маломощной радиосвязи не появились бы на рынке. Закон и бюрократия отразили бы этот удар цифровой армии.

Также не у дел осталась бы беспроводная связь. Технология должна была бы каким-то образом научиться использовать имеющийся диапазон частот более эффективно. Миниатюризация и цифровой принцип работы создали мир коммуникаций. История сотовой телефонии, беспроводного Интернета и многих других цифровых благ – это клубок из политики, технологий и законов. Невозможно распутать клубок, не вытягивая отдельные нити, но в будущем нити переплетутся еще более тесно.

От нескольких труб к миллионам флейт

Тридцать лет назад не было сотовых телефонов. Главы крупных компаний пользовались мобильными телефонами, но это были дорогие и громоздкие устройства. Миниатюризация превратила мобильный телефон из привилегии «больших шишек» в атрибут любого американского подростка. Но главное изменение произошло в *распределении частотного диапазона* – точнее, в способе его использования.

Во времена громоздких мобильных телефонов компания, обеспечивающая мобильную радиосвязь, должна была установить мощную антенну и получить от FCC право использовать диапазон частот в городской черте. Ведущий телефон (базовая станция) был небольшой радиостанцией, рассылающей широковещательный сигнал. Мобильный телефон должен был обладать достаточной мощностью, чтобы доставить сигнал базовой станции в пределах зоны покрытия. Технология мобильной связи по сути ничем не отличалась от радиосвязи и была двусторонней. Нехватка рабочих частот, по сей день остающаяся аргументом при необходимости ограничить число каналов, ограничивала количество мобильных телефонов. Министр Гувер предвидел это еще в 1922 году: «Очевидно, что если 10 миллионов телефонных абонентов будут пытаться докричаться в эфире до своих собеседников,... эфир станет чудовищным хаосом, исключающим какую бы то ни было связь».[1]

[1] *New York Times* от 28 февраля 1922 года.

Технология сотовой связи развивалась по закону Мура. Телефоны постоянно уменьшались, дешевели и убыстрялись. Поскольку обычное расстояние между базовыми станциями примерно полтора километра, для работы телефонов требуется незначительная мощность. Сигнал, принятый антенной, дальше передается по проводам – медным или оптоволоконным кабелям, протянутым на опорах или проложенным под землей. Необходима только ширина полосы частот, достаточная для обслуживания звонков внутри ячейки «сот» (области покрытия одной базовой станции), так что один и тот же диапазон может использоваться на всей территории работы сотовой связи. Чтобы предотвратить обрыв сигнала при перемещении из одной ячейки в другую, было разработано немало ухищрений, но в настоящее время компьютеры (в том числе микрокомпьютеры в самих телефонах) достаточно интеллектуальны, чтобы справиться с этой задачей.

Технология сотовой связи демонстрирует новое изменение способа использования диапазона радиочастот. Большинство систем радиосвязи в настоящее время работают на коротких расстояниях. Это связь между сотовым телефоном и базовой станцией. Между беспроводным маршрутизатором в закусочной «Starbucks» и ноутбуком клиента, попивающего кофе. Между трубкой и базой беспроводного телефона. Между ридером точки учета пользования платной высокоскоростной автострадой и электронным пропуском на ветровом стекле автомобиля. Между брелоком и блоком управления автосигнализацией. Между игровой консолью Wii и ее контроллером. Между док-станцией iPod, подключенной к прикуривателю, и автомобильным радиоприемником.

Даже спутниковое радио зачастую передается не со спутника в космосе, а с ближайшей антенны. В городах связи между спутником и приемником обычно мешают высотные здания, поэтому радиокомпании устанавливают повторители сигнала – дополнительные антенны, соединенные проводами. Слушая радиостанцию «XM» или «Sirius» в едущем автомобиле, вы, скорее всего, получаете сигнал с повторителя, расположенного в нескольких кварталах от вас.[1]

Диапазон радиочастот сегодня редко используется для передачи информации на дальние расстояния.

Диапазон радиочастот сегодня редко используется для передачи информации на дальние расстояния. Порядок присвоения частот был разработан во времена, когда радио главным образом применялось для связи типа «корабль-земля», передачи сигналов бедствия или вещания на большой территории. После того как большую часть страны опутали провода, большинство радиосигналов путешествуют лишь на несколько метров или сотен метров. Поэтому старые правила распределения частот уже не актуальны.

[1] Марк Ллойд (Mark Lloyd) «The strange case of satellite radio» (Странный случай со спутниковым радио), Центр американского прогресса, 8 февраля 2006 года.

Можно ли просто поделить диапазон на всех?

Некоторые технологические достижения позволяют лучше использовать частотный диапазон без изменения фундаментальной системы разделения полосы частот, показанной на рис. 8.1. Например, HD-радио сочетает несвязанный маломощный цифровой сигнал с аналоговыми сигналами СВ (AM) и FM. («HD» является торговой маркой. Не следует трактовать это название, как high definition – высокое разрешение.) Трансляция сигнала HD-радио в диапазоне СВ (AM) использует защитные полосы частот AM-станции для передачи абсолютно разного содержимого (рис. 8.3). Большинство приемников отфильтровывает защитные полосы, так что содержимое HD-радио не влияет на основной аналоговый сигнал, даже в виде шума. Для декодирования сигнала вещания HD-радио требуется специальный приемник.

HD-радио – это изящное решение, внедрение которого не встретило особых препятствий со стороны FCC. Комиссия смогла разместить в эфире еще больше радиостанций, которые могли позволить себе приобрести необходимое оборудование. Но базовая модель распределения диапазонов 1920-х годов осталась неизменной.

Даже присвоенные держателям лицензий полосы частот на практике могут оставаться недостаточно «загруженными». Как сказано об этом

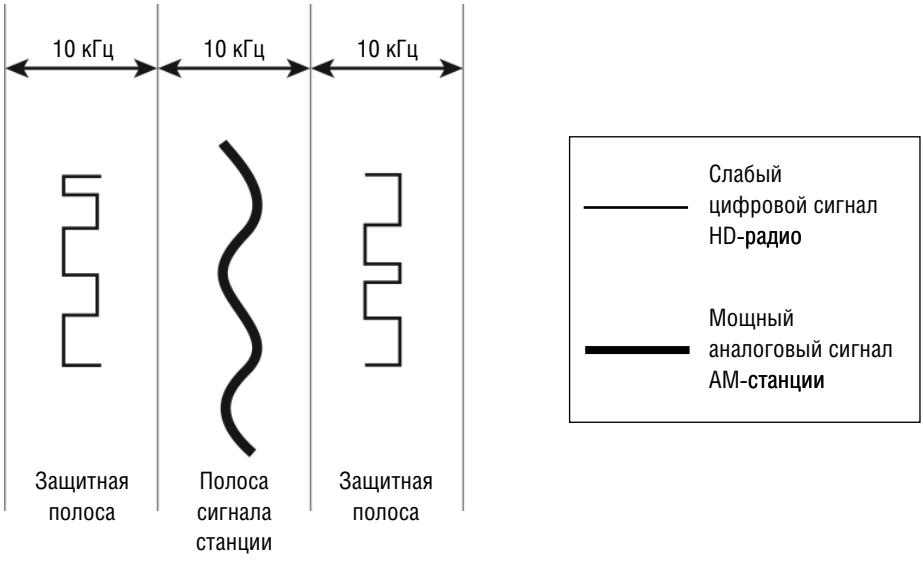


Рис. 8.3. *HD-радио передает маломощный цифровой сигнал в защитных полосах. В диапазоне СВ (AM) защитные полосы у обеих границ полосы частот, выделенной для обычной аналоговой станции, могут служить для независимой передачи цифрового сигнала, мощность которого настолько мала, что не влияет на основной сигнал*

в отчете FCC за 2002 год: «Ограниченность диапазона часто создает *проблему доступа к диапазону*. Свободные частоты есть, но их использование осложняется применением традиционных политик, основанных на традиционных технологиях».[1] К такому выводу комиссия пришла отчасти после прослушивания эфира на разных частотах, предпринятого для оценки использования частотного ресурса. Большую часть времени даже в густонаселенных городских образованиях, таких как Сан-Диего, Атланта и Чикаго, важные диапазоны почти на 100% не использовались. Если бы кто-то заполнил свободные частоты, он принес бы пользу обществу.

Около десяти лет комиссия экспериментировала со «вторичным рынком радиочастот». Участник, желающий получить часть диапазона во временное пользование, мог арендовать ее у владельца оригинальной лицензии, разумеется, за плату. К примеру, университетской радиостанции эфирное время нужно только иногда, днем по субботам, чтобы транслировать футбольные репортажи. Возможно, университет мог бы договориться с финансовой компанией, которой эфир не нужен, когда биржи закрыты.[2] Другой пример: можно использовать частоту, зарезервированную для сообщений об опасности. При этом вещание субарендаторов будет принудительно прерываться при широковещательной рассылке сигнала оповещения об опасности (что достигается настройкой оборудования).

Как показал пример интернет-аукциона eBay, подобный способ распределения товаров с помощью компьютера весьма эффективен. Использование определенных диапазонов частот в определенном регионе в определенное время может приносить выгоду, если владельцы оригинальных лицензий смогут эффективно организовать продажу части эфирного времени другим участникам рынка.

Но вторичный рынок не меняет базовую модель: частотный диапазон принадлежит в одно и то же время только одной станции. Идея «аукциона частот» подрывает основы модели. Вместо того чтобы одна полоса частот могла использоваться исключительно одной станцией, эта полоса делится на поддиапазоны и проводятся торги. В сущности, модель выдерживает сравнение полосы частот с земельными угодьями, которые можно разделить между всеми желающими попользоваться ресурсами.

---

[1] FRC, отдел политики использования частотного диапазона, отчет рабочей группы по эффективному использованию радиочастот от 15 ноября 2002 года.

[2] Марк Быковски и Майкл Маркус (Mark M. Bykowsky, Michael J. Marcus) «Facilitating spectrum management reform via callable/interruptible spectrum» (Облегчение реформирования управления диапазоном радиочастот при помощи отзываемого/прерываемого диапазона), Федеральная комиссия по коммуникациям, 13 сентября 2002 года.

Совместное использование диапазона

Изложив в 1943 году свой взгляд на события, судья Франкфуртер ненамеренно использовал аналогию, указавшую направление дальнейшего развития. Судья полагал, что диапазон частот – дефицитный ресурс: «Контроль радиосвязи вплоть до настоящего времени так же жизненно важен для ее развития, как контроль дорожного движения для развития автотранспорта».

Как и диапазон радиочастот, автомобильные дороги являются национальным достоянием. Федеральное и местное правительства контролируют их, устанавливая правила. Запрещается превышение скорости. Запрещается движение транспорта, габариты или масса которого превышают допустимые для данной дороги пределы.

При этом дороги принадлежат всем. Нет специальных шоссе только для правительства. Транспортная компания не может получить лицензию, позволяющую ей использовать какую-то дорогу, запрещая движение транспорта конкурентов. Автомобильные дороги доступны для всех, ограничиваясь лишь лимитом плотности движения.[1]

На сайте профессора Гарвардской школы права Йохая Бенклера (Yochai Benkler) www.benkler.org доступны для скачивания несколько познавательных статей, включая классическую «Преодоление агорафобии» («Overcoming Agoraphobia»). Более полно обсуждаемые темы раскрыты в его книге «Богатство сетей» («The Wealth of Networks»).

Дороги являются тем, что в науке права называется сервитутом, или «ресурсом общего использования» (об этом уже говорилось в главе 6). Океан также является сервитутом в отношении всемирного отлова рыбы. В теории, собственно, океан может не быть сервитутом. Рыболовецкие суда могли бы ловить рыбу в строго определенных участках океана. Если выделенная акватория обладает достаточными рыбными ресурсами, то рыбакам обеспечена безбедная жизнь. Но для общества в целом такое деление океана может быть совершенно неприемлемо. Океан лучше удовлетворяет нужды людей, если остается неделимым целым, конечно, при выработке адекватных квот на рыбную ловлю.

Вместо разделения диапазона можно его совместно использовать. В электронных коммуникациях есть прецедент. Интернет в целом является сервитутом. Пакеты пользователей смешиваются в потоки, движущиеся по световодам и радиоканалам центральных информационных магистралей Интернета. Пакеты кодируются. Отправитель

[1] Аналогия принадлежит Эли М. Ноам (Eli M. Noam), статья «Taking the next step beyond spectrum auctions: Open spectrum access» (Следующий шаг за аукционами диапазонов: открытый доступ к частотам), *www.columbia.edu/dlc/wp/citi/citinoam21.html.*

и адресат пакета выясняются на маршрутизаторах и конечных узлах. Конфиденциальная информация может быть зашифрована.

Нечто подобное можно проделать и с вещанием на радиоволнах – при условии, что стороны готовы по-новому осмыслить методы использования диапазона частот.[1] Две ключевых идеи: во-первых, использование множества небольших диапазонов не обязательно вызывает наложение соседних сигналов, так что можно значительно увеличить количество передаваемой информации; во-вторых, использование компьютеров в составе оборудования радиосвязи может существенно улучшить качество использования диапазона.[2]

Самый красивый изобретатель в мире

Системы связи с расширенным спектром открывались и переоткрывались несколько раз в разных странах.[3] Корпорации (ITT, Sylvania и Magnavox), университеты (особенно Массачусетский технологический институт) и государственные исследовательские лаборатории внесли свой вклад в разработку этого ключевого компонента современных систем связи (зачастую не подозревая о том, что работают в одном направлении).

---

[1] См., например, Лоуренс Лессиг (Lawrence Lessig) «Code and the Commons» (Шифр и ресурсы общего использования), доклад на основную тему на конференции Media Convergence 9 февраля 1999 года; Йохай Бенклер (Yochai Benkler) «The commons as a neglected factor of information policy» (Ресурсы общего использования как забытый фактор информационной политики), 26-я ежегодная конференция по телекоммуникациям, 3–5 октября 1998 года; Бенклер «Overcoming Agoraphobia» (Преодоление агорафобии), Harvard J. L. & Tech., 287 и «Property, commons, and the First Amendment» (Собственность, ресурсы общего использования и Первая поправка), доклад для Программы Первой поправки, Центр Бреннана по правосудию в Нью-йоркской школе права; Йон М. Пеха (Jon M. Peha) «Emerging technology and spectrum policy reform» (Развитие технологий и реформа политики использования радиочастот), Международный союз электросвязи (International Telecommunications Union, ITU), семинар по рыночным механизмам управления диапазоном радиочастот, Женева, январь 2007 года.

[2] За другими примерами можно обратиться к рабочей статье Кевина Вербаха (Kevin Werbach) «Open spectrum: the new wireless paradigm» (Открытый диапазон: новая парадигма беспроводной связи), Новый американский фонд, документы о радиосвязи, № 6, октябрь 2002 года.

[3] Роберт Шольц (Robert A. Scholtz) «The origins of spread-spectrum communications» (Изобретение связи с расширенным спектром), *IEEE Trans. Communications*, COM-30, № 5, май 1982 года, 822–853, COM-31, № 1, январь 1983 года, 82–84; Роберт Прайс (Robert Price) «Further notes and anecdotes on spread-spectrum origins» (Новые заметки и рассказы об изобретении связи с расширенным спектром), там же, 85–97; Роб Уолтерс (Rob Walters) «Spread Spectrum» (Расширенный спектр), Booksurge LLC, 2005 год.

Но наиболее примечательный случай в разработке систем связи с расширенным спектром – получение патента на изобретение голливудской актрисой Хэди Ламарр – «самой красивой женщиной в мире», по словам кинопродюсера Луиса Майера и авангардного композитора Джорджа Антейла.

Хэди Ламарр приобрела скандальную репутацию в Европе, снявшись обнаженной в фильме чешского режиссера Густава Махаты «Экстаз» в 1933 году (тогда актрисе было девятнадцать). Она вышла замуж за Фрица Мандла, австрийского поставщика вооружений, чьими услугами пользовались и Гитлер, и Муссолини. В 1937 году Хэди Ламарр сбежала от мужа и направилась сначала в Париж, а затем в Лондон. Там она встретилась с продюсером Луисом Майером и вместе с ним уехала в Голливуд. Хэди Ламарр стала звездой экрана и эталоном красоты для целого поколения (рис. 8.4).

В 1940 году актриса познакомилась с композитором Джорджем Антейлом. Ей хотелось улучшить фигуру, а Антейл также занимался женской эндокринологией, публикуя статьи в журнале «Esquire».[1] Поговорив о железах, актриса и композитор перешли к другим темам, в частности к торпедному вооружению.

Торпеда – то есть бомба с гребным винтом – может потопить мощный корабль. К исходу Первой мировой войны уже были разработаны радиоуправляемые торпеды, но качество управления оставляло желать лучшего. Эффективной мерой защиты от торпед была передача сильного шумового сигнала на управляющей частоте. При этом движение торпеды становилось непредсказуемым. Хэди Ламарр узнала все это, бывая на заводах своего первого мужа.

Актриса, всей душой желая союзникам победы, предложила идею передачи управляющего сигнала в виде коротких импульсов на разных частотах. Порядок смены частот должен быть записан в оборудовании как на самой торпеде, так и на управляющем корабле. Поскольку порядок смены частот неизвестен противнику, управление торпедой нельзя нарушить глушением сигнала в узком диапазоне. Глушение же всего возможного диапазона потребует чрезвычайно большой мощности.

Вклад Джорджа Антейла заключался в идее управления сменой частот при помощи устройства, подобного механизму пианино, – композитор отлично разбирался в этом; его самое известное произведение («Механический балет») было написано для синхронно играющих пианистов. Разработанное Джорджем Антейлом и Хэди Ламарр устройство управления (никогда не применявшееся) могло работать на 88 часто-

[1] Джордж Антейл (George Antheil) «Glands on a hobby horse»(Эндокринология как хобби), *Esquire*, апрель 1936 года, 47; «Glandbook for the questing male» (Эндокринология для интересующихся мужчин), май 1936 года, 40; «The glandbook in practical use» (Практическая эндокринология), июнь 1936 года, 36.

Рис. 8.4. *Хэди Ламарр примерно в те годы, когда она совместно с Джорджем Антейлом предложила идею управления по радиосвязи с расширенным спектром*

© Цифровой архив Bettmann корпорации CORBIS

тах – столько клавиш имеется на пианино. Корабль и торпеда должны были иметь идентичные пианинные валики и, применяя их согласно патенту, шифровать управляющий сигнал.

История изобретения Хэди Ламарр и Джорджа Антейла, а также роль изобретения в разработке систем связи с расширенным спектром описаны в книге Роба Уолтерса (Rob Walters) «Spread Spectrum» (Расширенный спектр) .

В 1941 году Хэди Ламарр и Джордж Антейл представили свой патент (рис. 8.5) в Управление военно-морского флота США. В небольшой заметке в рубрике «Развлечения» газеты *New York Times*[1] армейский инженер описывал совершенно патентное изобретение, которое «относится

[1] «Hedy Lamarr Inventor» (Изобретатель Хэди Ламарр), *New York Times* от 1 октября 1941 года, 24.

UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.

An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

Fig. 2 is a schematic diagram of the apparatus at a receiving station;

Fig. 3 is a schematic diagram illustrating a starting circuit for starting the motors at the transmitting and receiving stations simultaneously;

Fig. 4 is a plan view of a section of a record strip that may be employed;

Fig. 5 is a detail cross section through a rec-

Рис. 8.5. *Патент на изобретение системы связи с расширенным спектром Хэди Ламарр (на патенте указано имя Хэди Кейслер Марки: Кейслер – девичья фамилия, Марки – фамилия второго мужа из шести, Ламарр – сценический псевдоним) и Джорджа Антейла. Слева: начальная страница патентного документа. Справа: схема механизма с пианинным валиком, иллюстрирующая патент*

Патентное бюро США

к управлению военным оборудованием на расстоянии». Тем не менее, флот не спешил воспользоваться новой разработкой. Хэди Ламарр взялась за продажу облигаций военного займа. Называя себя «всего лишь золотоискателем для Дяди Сэма», актриса продавала поцелуи, и на одном обеде собрала 4,5 миллиона долларов. Ромуальд Иренеус Сцибор-Мархоцкий, инженер, работавший на военно-морской флот в середине 1950-х, обнаружил патент, решая задачу обнаружения подводных лодок противника. Инженер не узнал изобретателя, потому что патент был подписан настоящей фамилией, а не сценическим псевдонимом.[1]

Такова, вкратце, эта удивительная история изобретательности, совместной работы, патриотизма и жажды славы, завершившаяся созданием нового метода радиосвязи. Работа Хэди Ламарр и Джорджа Антейла была оценена по достоинству только в 1990-х. К этому времени подобные разработки появились и у военных инженеров. Хэди Ламарр, изобретатель по воле случая, для неисследованной территории была скорее Лейфом Эрикссоном, чем Кристофором Колумбом. В 1997 году Фонд электронной безопасности отметил работу Хэди Ламарр премией. «Очень своевременно», – пошутила актриса. На вопрос о том, какое из достижений для нее наиболее ценно, актриса ответила: «Фильмы принадлежат своему времени. Технология вечна».

Емкость канала

Хэди Ламарр и Джордж Антейл открыли частный способ использования широкополосного сигнала – его «расширение» по частотному спектру. Полное теоретическое исследование систем связи с расширенным

[1] *www.rism.com/*

спектром стало одним из наиболее выдающихся математических достижений Клода Шеннона в конце 1940-х. Тогда еще не было цифровых телефонов или устройств радиосвязи, подобных современным. Клод Шеннон открыл базовые законы, которые сделали возможным появление цифровых коммуникаций. Теорема Шеннона-Хартли для разработки систем связи с расширенным спектром имеет то же значение, что уравнения Максвелла – для открытия радиоволн.

Выводы Шеннона (основанные на работе Ральфа Хартли, проделанной за два десятилетия до исследований Шеннона) подтвердили, что «интерференция» – не совсем точный термин для описания взаимодействия нескольких одновременных сигналов и оценки информационной емкости канала связи. Сигналы могут передаваться на одной частоте и быть разделены на другом конце достаточно интеллектуальным приемным устройством.

Инженеры всегда считали, что ошибки в связи неизбежны. Передача битов по кабелю или в эфире невозможна без потери той или иной доли информации. Предполагалось, что количество ошибок можно уменьшить, понизив скорость передачи данных, – как человек замедляет речь для более четкого понимания. Однако гарантировать полное отсутствие ошибок невозможно.

Ошибки и задержки

Хотя количество ошибок при передаче можно снизить почти до нуля, полностью исключить их невозможно. И все же ошибка менее вероятна, чем, к примеру, гибель получателя информации от землетрясения (см. приложение). Гарантировать точность доставки можно, добавляя в сигнал избыточную информацию – нечто вроде упаковки почтовых посылок в тару, предохраняющую от повреждения. Приближение скорости передачи данных к «границе Шеннона» предполагает специальное кодирование битов сообщения. Кодирование может породить временную *задержку*, необходимую для «упаковки» и пересылки кодированных битов. Задержка может быть проблемой, например, для голосовой связи, поскольку раздражает собеседников. К счастью, телефонные звонки не требуют избыточного кодирования – люди могут примириться с некоторой долей помех.

Клод Шеннон показал, что каналы связи можно использовать иначе. Любой канал связи имеет определенную *информационную емкость* – количество бит, которые можно передать в единицу времени. Если провайдер заявляет, что предоставляет вам интернет-соединение с скоростью 3 Мбит/с (3 миллиона бит в секунду), то это и есть информаци-

онная емкость канала связи между вами и оборудованием провайдера (точнее, она должна быть такой – не следует слепо верить рекламе). Если рассматриваемое соединение реализовано в виде подключения по телефонной линии и вы перейдете на оптоволоконное, то информационная емкость канала должна еще возрасти.

Какой бы емкостью ни обладал ваш канал, у него есть одно важное, доказанное Клодом Шенноном свойство: биты могут передаваться по каналу связи от источника к приемнику *со сколь угодно малым уровнем ошибки* до тех пор, пока скорость передачи не превосходит информационную емкость канала. Любая попытка превышения допустимой скорости неизбежно приведет к потере данных. Пока скорость передачи остается в допустимых пределах, возможно такое кодирование данных, которое сведет вероятность искажений сигнала почти к нулю. Ошибки неминуемы, только если скорость передачи превышает емкость канала.

Мощность, сигнал, помехи и полоса пропускания

Емкость радиоканала зависит от частот, на которых передаются сообщения, и от мощности сигнала. Уместно рассмотреть эти факторы по отдельности.

Радиосигнал в действительности никогда не передается на одной частоте. Сигнал всегда использует *диапазон* частот для передачи звуковых колебаний. Одна частота может нести только сигнал одного тона. *Полоса пропускания* радиовещания – это ширина радиодиапазона, то есть разница между верхней и нижней граничными частотами. Министр Гувер первоначально выделил для каждой станции полосу пропускания в 10 кГц.

Если вы можете переслать некоторое число битов в секунду в заданной полосе пропускания, то при расширении полосы вдвое вы сможете пересылать вдвое больше битов. Две операции передачи могут совершаться одновременно, не пересекаясь. *Таким образом, информационная емкость канала пропорциональна полосе пропускания.*

Полоса пропускания

Поскольку емкость канала зависит от полосы частот, термин «полоса пропускания» иногда используется в значении «количество информации, передаваемой за секунду». Однако с технической точки зрения корректно считать термин «полоса пропускания» относящимся к области электромагнитной связи, но и тогда пропускная способность – не единственный фактор, определяющим емкость канала связи.

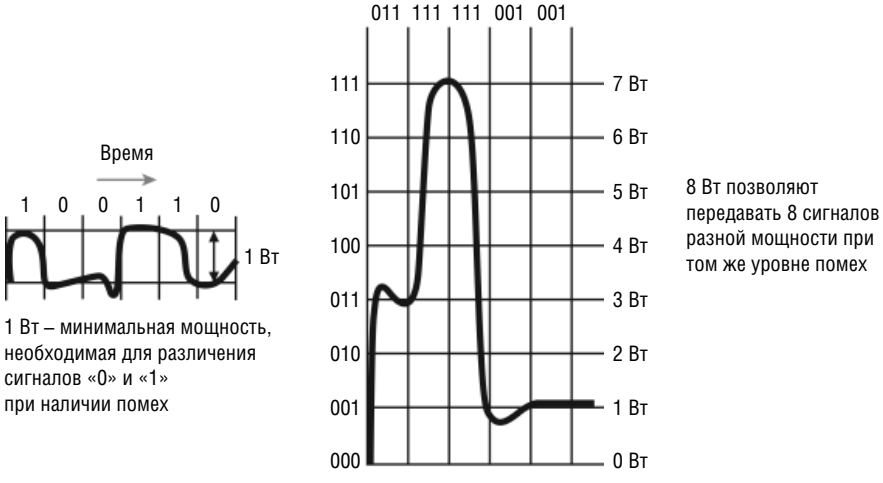


Рис. 8.6. *Закон Шеннона-Хартли. Уровни мощности разных сигналов должны достаточно отличаться, чтобы исключить ошибки приема в условиях помех. Для утроения скорости передачи битов канала требуется восемь уровней мощности*

Соотношение с мощностью сигнала несколько иное. Для простоты предположим, что вы можете передать один из двух возможных сигналов, «0» или «1», за одну секунду. Если вы можете *увеличить мощность, оставляя неизменной полосу пропускания или временной интервал*, то сколько сигналов вы сможете передать?

При передаче значения «0» и «1» можно представить сигналами разной мощности. Для простоты предположим, что значению «0» соответствует нулевая мощность, а значению «1» – мощность 1 Вт. Чтобы различать сигналы, приемник должен быть достаточно чувствительным, чтобы отличить 0 и 1 Вт. Помехи – например, от солнечных вспышек в ионосфере – также должны быть достаточно слабыми, чтобы исключить ошибку принятия сигнала типа «0» за сигнал типа «1».

С теми же условиями четыре уровня мощности позволяют передать за то же время (например, за одну секунду) два бита. Мощность 0 Вт соответствует паре битов 00, 1 Вт – 01, 2 Вт – 10, 3 Вт – 11. Чтобы исключить ошибку, каждый уровень мощности сигнала должен отличаться от соседнего не меньше, чем на 1 Вт. Если уровни мощности слишком близки, то помехи при передаче могут создать ошибки при приеме. Чтобы одновременно передать три бита, придется задействовать восемь уровней мощности – от 0 до 7 Вт. Таким образом, с увеличением количества одновременно передаваемых битов необходимая мощность возрастает экспоненциально (рис. 8.6).

Итак, из закона Шеннона-Хартли следует, что *емкость канала зависит и от ширины полосы пропускания, и от мощности сигнала, при-*

чем для увеличения емкости предпочтительнее расширять полосу. Для сравнения: расширение полосы пропускания в десять раз даст такой же эффект, как и увеличение мощности сигнала в тысячу раз ($2^{10} = 1024$)! Полоса пропускания действительно ценный ресурс.

Для одного сигнал, для другого помеха

Следствия из закона Шеннона-Хартли о решающем влиянии ширины полосы пропускания на емкость канала могут быть поистине поразительными. Если бы радиостанция WBZ со своим передатчиком в 50 кВт получила для вещания полосу в 100 кГц вместо положенных по Акту о радио 10 кГц, то на коротких расстояниях станция могла бы транслировать то же количество информации, используя передатчик, сравнимый по мощности с электрической лампочкой.

Конечно, одна станция не может получить в исключительное пользование полосу в 100 кГц. Деление диапазона радиочастот даже на полосы по 10 кГц быстро приводит к дефициту свободных частот. Системы связи с расширением спектра работают, только если считать весь радиодиапазон ресурсом общего использования. Но для того чтобы понять последствия вещания множества сигналов в одном диапазоне, требуется более тщательное исследование.

Уровень мощности, влияющий на емкость канала радиосвязи, в сущности является не собственно мощностью сигнала, а соотношением между мощностью сигнала и мощностью помех – так называемое *соотношение сигнал-шум*. Другими словами, если десятикратно понизить уровень помех, то можно уменьшить мощность передатчика с 10 до 1 Вт, сохраняя ту же скорость передачи данных.

Помехами («шумом») могут быть *сигналы других передатчиков*. Не имеет значения, идут помехи от другого передатчика или от космических объектов. Все станции, вещающие в одном диапазоне, должны каким-то образом бороться с эквивалентным уровнем собственных помех.[1]

С популярными расчетами параметров широкополосного радиовещания можно ознакомиться в статье Дэвида Хьюза и ДиВэйна Хендрикса (David Hughes, DeWayne Hendricks) «Spread-Spectrum Radio» (Радиосвязь с расширенным спектром), журнал «Scientific American», апрель 1998 года, с. 94–96).

[1] Поэтому в современных работах по теории информации используют обозначение I (interference – интерференция, перекрывание) вместо N (noise – шум). Сигнал одного источника может являться шумом для другого; с точки зрения физики, все это – лишь интерференция сигналов.

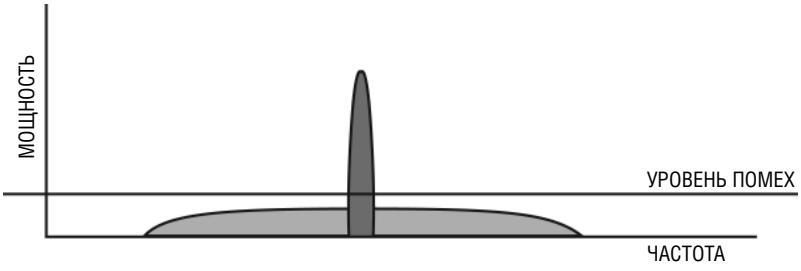


Рис. 8.7. *Принцип широкополосного вещания. Одинаковая скорость (площадь закрашенной области) передачи данных при значительном снижении мощности может быть достигнута путем расширения полосы частот, даже если уровень полезного сигнала ниже уровня помех*

Еще одно удивительное следствие закона Шеннона-Хартли: *безошибочная передача данных возможна даже в условиях, когда уровень мощности помех выше уровня мощности полезного сигнала.*

К примеру, на шумной вечеринке вы все еще можете общаться с кем-то, если сосредоточитесь именно на его голосе, даже если голос тише, чем окружающий шум. Но закон Шеннона-Хартли дает гораздо больше: *снижение скорости передачи данных позволит исключить ошибки приема даже в том случае, когда мощность помех многократно превышает мощность полезного сигнала. При достаточной ширине полосы пропускания можно значительно понизить мощность передачи, не снижая скорость* (рис. 8.7). То, что может показаться другим всего лишь шумами, в действительности может нести в себе полезный сигнал.

Теорема Шеннона-Хартли – это математическая жемчужина. Теорема показывает теоретические пределы возможного, но не сообщает, как этого можно достичь на практике. Как формула Эйнштейна $E = mc^2$, ни о чем не говорящая непосвященному, описывает происходящее внутри атомного реактора или ядерной бомбы. Изобретение Хэди Ламарр могло быть использовано на практике, однако в конце XX века появились новые остроумные инженерные решения, порой с весьма странными названиями.

Между теоретическими выкладками Ральфа Хартли и Клода Шеннона и практической реализацией систем связи с расширенным спектром было два основных препятствия. Первое – состояние технологии: чтобы обеспечить передачу потребителям цифрового высококачественного видео и звука, компьютеры должны были стать достаточно быстрыми, мощными и дешевыми (они появились только в 1980-х). Второе – законодательство и бюрократия. Это препятствие не зависит ни от математики, ни от технологии. Чиновничий аппарат реагирует намного медленнее, чем развиваются технологии.

Радиодиапазон для всеобщего пользования

Сегодня в каждой закусочной «Starbucks» есть беспроводной доступ в Интернет, типа WiFi. Гостиничные номера, студенческие общежития и многие частные дома тоже подключены к беспроводной связи. Это стало возможным потому, что небольшой отрезок полосы частот – меньше миллиметра на рис. 8.1 – стал общедоступным, чем и воспользовались творчески настроенные инженеры. Это пример того, как принцип общего использования стимулирует развитие технологии, а также того, что нынешние хозяева диапазона предпочитают оставаться в своем привилегированном положении.[1] Если государство примет мудрые решения, то еще большая часть радиодиапазона со временем станет доступна всем желающим.

Майкл Маркус стал «случайным революционером». Он получил диплом инженера-электрика в Массачусетском технологическом институте. Во время войны во Вьетнаме служил в ВВС США. Там офицер Маркус работал над системой обнаружения подземного ядерного взрыва. В это время еще не было Интернета – только его предшественница, военная сеть ARPANET. По окончании срочной службы Майкл Маркус начал работать в мозговом центре Пентагона, исследуя потенциальные возможности военного применения новых средств связи.

Летом 1979 года Майкл Маркус присоединился к группе разработки электронного оборудования для вооруженных сил США. Как обычно в армии, присутствующих рассадили по алфавиту. Рядом с Майклом Маркусом сидел Стив Лукасик, ведущий исследователь FCC. Во время разработки сети ARPANET Стив Лукасик работал директором Агентства по перспективным научно-исследовательским разработкам (ARPA), а после этого стал специалистом по сети ARPANET в компании Xerox. Он пришел работать в комиссию (которая обычно не занималась новыми исследованиями), потому что администрация президента Картера в это время считала существующее федеральное законодательство тормозом прогресса. Исследователь спросил у Майкла Маркуса, что он думает о перспективных направлениях в радиосвязи. Помимо прочего, ответ содержал фразу «широкополосная связь». Это был ответ инженера, но, к сожалению, не политика.

Армия предпочитает хранить секреты, и возможности широкополосной связи были мало известны гражданскому населению. FCC запретила гражданское использование широкополосной связи испытанным десятилетиями способом – запретом выделения одному лицу или организации достаточно широкого диапазона частот. Использование широкополосной связи независимо от уровня мощности было нарушением закона. Лукасик предложил Маркусу работать в комиссии, защищая развитие систем широкополосной связи и других инновационных тех-

[1] Веб-страница «Early civil spread spectrum history» (Начало истории гражданской широкополосной связи), *www.marcus-spectrum.com/SSHistory.htm*.

нологий. Эта работа потребовала кардинального изменения методов работы комиссии.

Вскоре после создания Федеральной комиссии по радиосвязи (FRC) Соединенные Штаты поразила Великая депрессия. В 1970-х Федеральная комиссия по коммуникациям (FCC) все еще жила воспоминаниями о второй четверти XX века, в то время как национальная экономическая политика тяготела к регулированию свободного рынка. Как правило, изобретатели ненавидят контроль, а капиталисты, напротив, чувствуют себя превосходно, когда закон защищает их интересы. В мире радио, где частотный спектр является дефицитным, необходимым, подконтрольным правительству ресурсом, эти движущие силы обладают огромной и опасной мощью.[1]

Силы радиоэфира, такие как уже существующие теле- и радиостанции и сотовые операторы, в прошлом получили от правительства свою долю спектра частот и без труда продлевают свои «права».[2] Ни одна из этих сил, естественно, не желает, чтобы «ее» полоса частот была отдана под инновации, которые могут представлять угрозу привычному бизнесу. Разработчики новых перспективных технологий не могут продолжать свою деятельность без гарантии государства, что им предоставят нужную полосу частот, а инвесторы не хотят вкладывать деньги в разработки, основанные на ресурсах, которыми владеет правительство и которые оно же может в любой момент отобрать.

Власти охотно принимают общественные предложения об ослаблении правил, но, как правило, слышат только тех, у кого достаточно средств, чтобы пролоббировать свои запросы. И эти запросы, разумеется, не в пользу изменений. Силы, контролирующие мир радио, пугают правительство предсказаниями грядущих катастроф. Фактически владельцы крупных станций в своих жалобах часто «приукрашивают» прогнозы конца света в надежде исключить конкуренцию. В результате власти забывают о своей главной обязанности – действовать во благо общества, а не ради прибылей акул радиобизнеса. Властям легче предоставить события самим себе.

Чиновники могут авторитетно заявлять, что учитывают все мнения, а не только те, что вызваны большими затратами на путешествия и лоббирование. Законы, призванные предотвращать взаимные помехи соседних сигналов, стали предотвращать добросовестную конкуренцию.

---

[1] Дебора Спар (Debora L. Spar) «Ruling the Waves» (Управляя волнами), Harvest, 2003 год; также презентация Майкла Маркуса, *collegerama.tudelft.nl/mediasite/Catalog/?cid=73e977a6-0283-4ee6-9813-a61df0dd1778*.

[2] Забавно, что власти сохраняют нормы, которые использовались до начала регулирования использования радиочастот. Главные корпорации, выигравшие в то бесконтрольное время, теперь зависят от государственного законодательства, которое их защищает.

Здесь есть еще одно препятствие. Большая часть работ в области систем связи принадлежит коммерческому сектору. Сотрудники FCC знают, где их будущее – в коммерческом использовании диапазона. Сотни рядовых и руководящих сотрудников комиссии, включая всех восьмерых бывших директоров, представляли или работали на бизнес, который должны были контролировать.[1] Эти подвижки из правительственной работы в коммерческую занятость не нарушают этику госслужбы. Однако руководство комиссии может оказаться перед выбором: недовольство потенциального крупного работодателя или разочарование малоприбыльным проектом или вовсе безденежным некоммерческим предприятием. Неудивительно, что работники FCC хорошо помнят, кто может предложить им средства к существованию после окончания работы на правительство.

В 1981 году Майкл Маркус и его коллеги внесли предложение разрешить маломощное вещание в широком диапазоне частот.[2] Почти все владельцы лицензий на охваченные предложением поддиапазоны тут же запротестовали. FCC пошла на попятную и, пытаясь найти выход из тупика, начала исследовать радиодиапазон в поисках неких свободных частот.

Поиск производился по трем так называемым мусорным частотам (они использовались только для «промышленных, научных и медицинских» целей). К примеру, в микроволновых печах применяется электромагнитное излучение с частотой около 2,45 ГГц. Против этого никто не возражал: излучение печей может проникать за их пределы, поэтому индустрия телекоммуникаций данную частоту не использовала.[3]

Корпорации RCA и General Electric возражали против маломощного широкополосного вещания в любой его форме, но их доводы были сочтены преувеличенными. Пробный диапазон был разрешен в 1985 году для экспериментальной широкополосной передачи информации с условием, что для исключения интерференции сигналов будет применяться динамическая смена частот или подобная технология.

---

[1] Центр общественного единства (Center for Public Integrity), «Networks of Influence» (Сети влияния), 28 февраля 2004 года.

[2] В правилах и нормативах FCC больше нет лицензирования радиочастот и других широкополосных излучений, Gen Docket № 81-413, 15 сентября 1981 года, *www.marcus-spectrum.com/documents/SpreadSpectrumNOI.pdf*. Эти сведения основаны на отчете корпорации MITRE «Потенциальное использование технологий широкополосной связи в неправительственных организациях» («Potential use of spread spectrum techniques in non-government applications»), декабрь 1980 года, *www.mitre.org/work/tech_papers/tech_papers_07/MTR80W335/MTR80W335.pdf*.

[3] «A brief history of Wi-Fi» (Краткая история Wi-Fi), *Economist* от 10 июня 2004 года.

Майкл Маркус еще толком не знал, что можно было бы разработать, но многие инженеры поспешили не упустить предоставившиеся возможности. Ирвин Джекобс через несколько месяцев основал компанию QUALCOMM – к 1990 году фирменная технология мобильной связи CDMA уже пользовалась широкой популярностью. Несколько лет спустя компания Apple Computer и другие производители компьютерного оборудования на основе стандартов FCC разработали устройства для создания широкополосных беспроводных локальных сетей – беспроводные маршрутизаторы (разработка компании Apple вышла под торговой маркой Airport). В 1997 году, когда комиссия одобрила семейство стандартов беспроводной связи IEEE 802.11 и освободила диапазоны для них, даже пресса едва обратила на это внимание.[1] В течение трех последующих лет беспроводные сети проникли повсюду, и в настоящее время многие персональные компьютеры поставляются с поддержкой беспроводной связи типа WiFi.

За свои усилия Майкл Маркус был отправлен во «внутреннюю ссылку» на семь лет, но в эпоху Клинтона вернулся к работе над системами широкополосной связи. В настоящее время Майкл Маркус на пенсии, работает независимым консультантом.

На сайте Майкла Маркуса (*www.marcus-spectrum.com*) есть интересные материалы и мнения по предоставлению общественности права использования части радиодиапазона, а также по истории развития систем широкополосной связи.

Успех технологии WiFi дал «зеленый свет» и более радикальным разработкам. Наиболее экстравагантная из них – сверхширокополосная связь (ultra wide band, UWB). Сверхширокополосная связь возвращает нас во времена, когда Генрих Герц поставил свой знаменитый опыт с обнаружением радиоволн, вызванных мощными электрическими разрядами во всем диапазоне частот. Здесь, однако, есть два важных отличия. Во-первых, современная сверхширокополосная связь использует очень слабый сигнал в сверхширокoм диапазоне, чтобы избежать искажения любых других возможных сигналов. Во-вторых, формируются чрезвычайно короткие и тщательно синхронизированные импульсы, что позволяет обеспечить передачу цифрового сигнала. Такая связь

[1] Одна из немногих газетных статей, отметивших появление технологии WiFi: «FCC OK's short-range wireless communications» (FCC разрешила использовать широкополосную связь малого радиуса), *Chicago Sun-Times* от 10 января 1997 года, 50. Напротив, аукцион диапазонов для сотовой связи освещался почти в каждом деловом издании 14 или 15 января.

ограничена несколькими метрами, но в этих пределах может передавать данные с очень высокой скоростью. Представьте, что больше не нужно возиться с проводами, соединяющими цифровой телевизор, приемник кабельного ТВ и DVD-проигрыватель. Представьте, как из вашей домашней аудиосистемы цифровая музыка передается в автомобильную аудиосистему, прямо в гараж. Вообразите беспроводной видеотелефон, работающий быстрее и лучше обычной трубки. Возможности не ограничены... если правительственный контроль продолжит снижаться.

Что ждет радиосвязь в будущем?

Радиосвязь, как и все направления цифровой экспансии, не стоит на месте. Но технологии связи совершенствуются не так быстро, как компьютерное видео, распознавание голоса или предсказание погоды. Причина – негибкий правительственный контроль. Настоящее снижение государственного давления еще только набирает обороты.

Если бы радиоустройства были интеллектуальными

Расширение спектра – пример рационального использования частотного диапазона. Сравнение предельно простого устройства обычных радиоприемников и изощренной архитектуры компьютеров приводит и к другому рациональному решению. Если бы можно было перенести их в прошлое, современные приемники легко бы ловили сигнал станций восьмидесятилетней давности, а приемники того времени успешно воспроизводили бы трансляцию современных передатчиков, скажем, в диапазоне средних волн. Такая обширная «обратная совместимость» стоит значительной доли эффективности. Но истинная причина совместимости – не в огромном количестве работоспособных устройств, а в том, что силы, контролирующие мир радио в интересах сохранения своей доли рынка, *постоянно* препятствуют такому совершенствованию приемников, которое позволило бы принимать (и разместить в диапазоне) больше станций.

Если бы радиоустройства были интеллектуальными и активными, вместо того чтобы быть предельно простыми устройствами пассивного типа, радиосвязь предоставляла бы намного больше информации.

Если бы радиоустройства были интеллектуальными и активными, вместо того чтобы быть предельно простыми устройствами пассивного типа, радиосвязь предоставляла бы намного больше информации. Вместо трансляции со станции на высокой мощности, требуемой для передачи сигнала на дальние расстояния к пассивным приемникам, ретранслировать получаемый сигнал могли бы маломощные приемники. Запросы на нужную информацию можно было бы передавать от приемника к приемнику. Совместно приемники могли бы принимать более насыщенный сигнал, чем каждый по отдельности. Или несколь-

ко маломощных станций объединились бы, чтобы создать один мощный сигнал, доступный для приема на дальних расстояниях.

Подобная «командная работа» уже применяется в *сетях беспроводного мониторинга*. Маломощные компьютеры, оснащенные устройствами радиосвязи с датчиками, могут осуществлять сбор информации, например о температуре или сейсмической активности. Такие устройства можно устанавливать в неблагоприятной среде, такой как кратер проснувшегося вулкана или антарктическая колония пингвинов исчезающего вида. С минимальными затратами мощности, обеспечивая безопасность исследователей, устройства мониторинга могут собирать информацию и передавать ее на общий высокомощный передатчик.

Что значит «интеллектуальное» устройство?

«Интеллектуальное», или «умное», радио известно под разными техническими обозначениями. Два наиболее часто используемых обозначения – «программно управляемое радио» (software-defined radio, SDR) и «когнитивное радио» (cognitive radio). Первый термин относится к устройствам, которые можно перепрограммировать, чтобы изменить рабочие характеристики (например, рабочий диапазон – СВ или УКВ – или тип модуляции). Второй термин обозначает радиоустройства, в которых для увеличения эффективности использования полосы частот применяются элементы искусственного интеллекта.

«Интеллектуальные» радиоустройства могут существенно расширить объем вещания, если будет ослаблен удушающий контроль законодательства и появятся новые стимулы для инноваций.[1]

Есть и другая причина развивать «интеллектуальную» радиосвязь. Даже в существующей «узкополосной» модели распределения частот, когда каждый сигнал занимает небольшой отдельный диапазон, недорогие вычислительные системы могут улучшить положение. Устоявшееся мнение о том, что предотвращение интерференции сигналов – забота правительства (со вступления в силу Акта о радио 1912 года), давно устарело.

Радиоволны не пересекаются, не подавляют друг друга, подобно отдельным людям в толпе: волны взаимно проникают друг в друга. Если две волны проходят по антенне типичного радиоприемника, ни один из сигналов нельзя воспринять отдельно.

---

[1] Дэвид Рид (David Reed) «The sky's no longer the limit» (Неба хватит на всех), *Context Magazine*, зима 2002–2003 гг.

Чтобы лучше понять, о чем идет речь, попросите мужчину и женщину встать позади вас и начать читать разные книги с одинаковой громкостью. Если вы не сфокусируетесь, то услышите только невнятный шум. Но если вы сосредоточитесь на одном из голосов, то сможете выделить его и разобрать слова. Это возможно, потому что вы подключили систему обработки сигналов вашего мозга. Мозг может отличить женский голос от мужского. Имея доступ к словарному запасу, мозг попытается выделить отдельные слова. Радиоприемник в принципе сможет делать то же самое – если не сегодня, то сможет в недалеком будущем, когда компьютеры станут более мощными.

Но здесь нас ждет замкнутый круг наподобие известного вопроса о курице и яйце. Зачем покупать «интеллектуальный» приемник, если нет соответствующего сигнала вещания? Вещания не будет, пока кто-то не решится вложить в дело капитал. Инвесторы не станут вкладывать средства в проект, который покоится на зыбкой почве туманных распоряжений FCC. Производство пассивных радиоприемников и установку неэффективных передатчиков спонсируют акулы рынка, они же лоббируют нужное им законодательство.

Более того, гиганты индустрии телекоммуникаций и развлечений – одни из главных жертвователей избирательных кампаний по формированию состава Конгресса. Члены Конгресса часто оказывают давление на комиссию, чтобы та шла против интересов общества и навстречу интересам спонсоров. Эта проблема была очевидна еще в 1930-х, когда законодательство о радиосвязи только начинало формироваться: «Ни один квазиправовой орган государства еще не подвергался столь мощному давлению со стороны Конгресса, как FRC».[1] Принцип действия незыблем.

Телевидение, развлечения и Конгресс

Во время выборов 2006 года в Конгресс США индустрия телекоммуникаций и развлечений вложила в кампании перевыборов более 12 миллионов долларов – больше, чем нефте- и газоперерабатывающая промышленность. Три наиболее крупных жертвователя – корпорации Comcast и Time Warner и Национальная ассоциация кабельного телевидения (National Cable & Telecommunications Association).[2]

---

[1] Лоуренс Шмекебиер (Laurence F. Schmeckebier) «The Federal Radio Commission» (Федеральная комиссия по радиосвязи), Брукингский институт, Институт правительственных исследований, издания Правительства США, № 65, 55.

[2] *opensecrets.org/industries/mems.asp*

Другие технологии, такие как разработка персональных компьютеров, не попадали в этот замкнутый круг. Любой желающий внедрять инновации должен получать прибыль. Инвесторы придерживают капиталы в зависимости от качества технологии и ее востребованности на рынке, а не от реакции федеральных властей. Чрезмерно усиленная защита прав на интеллектуальную собственность подавляет творческую мысль, как показано в главе 6, но в проблеме виноваты законодатели, не сотрудники комиссии.

Законодательство само создает дефицит ресурсов, чтобы оправдывать им еще более строгие меры!

Беспроводные технологии связи, от сотовых телефонов до брелоков управления автосигнализацией, привлекают внимание общественности и востребованы на рынке. Для поощрения инноваций необходимо сломать законодательные барьеры в области радиосвязи, в частности, широкополосных систем. Законодательство само создает дефицит ресурсов, чтобы оправдывать им еще более строгие меры!

Нужна ли нам цифровая экспансия?

Технологии имеют свойство объединяться. В 1971 году профессор компьютерных наук и прикладной математики Гарвардского университета Энтони Эттингер предвидел, что технологии обработки данных и коммуникаций движутся навстречу друг другу. Профессор Эттингер назвал новое направление «компуникацией». Современные пользователи иногда не осознают того, что их данные хранятся где-то в тысячах километров от места назначения, пока не разорвется интернет-соединение. Телефонное оборудование первоначально соединялось медными проводами, а телевизионные станции обычно транслировали передачи по электромагнитным волнам, а сегодня большая часть телефонных звонков передается по радиосвязи, а телевизионное вещание – по кабелям.

Законы, правила, бюрократия изменяются намного медленнее, чем контролируемые ими технологии. В FCC все еще два отдельных бюро – по проводной и беспроводной связи. К широковещательному телевидению и радио применяются специальные законы об ограничении содержимого, хотя само понятие «широкого вещания» уже можно считать инженерным анахронизмом.

Разветвленная организация правовых структур тормозит развитие современных многоуровневых технологий. Контроль уровня содержимого не должен основываться на устаревшем понимании технических ограничений уровня физической реализации. Инвестиции в развитие уровня реализации не должны давать инвесторам возможность контролировать уровень содержимого. Интерес общества – на стороне инноваций и эффективности, а не в продлении существования устаревших технологий и круговой поруке тех, кто контролирует, с теми, кто представляет эти технологии.

Но если диапазон радиочастот наконец-то будет доступен для всех инноваций и станет использоваться более эффективно, чем сейчас, с увеличением числа каналов и прочим, – удовлетворит ли результат общество?

Существуют общие экономические и социальные преимущества от инноваций в технологиях беспроводной связи. Устройства для управления приводом гаражных дверей, игровые приставки и ридеры платных автострад не спасают жизни, конечно, но это могут сделать беспроводные датчики пожарной сигнализации и системы глобального позиционирования. История технологии WiFi служит неплохим примером того, как быстро новая разработка может стать важным элементом как деловой, так и персональной инфраструктуры.

А что же телевидение и радио? Станет ли обществу лучше, если вместо 13 каналов, как было в 1950-х, или нескольких сотен, как сейчас, будут доступны миллионы каналов вещания? Не чревато ли такое изобилие источников всеобщим снижением качества содержимого вещания и социальным разобщением, когда каналы с качественной достоверной информацией фактически будут задавлены общей массой? Можно ли будет сдерживать поток непристойностей, которые многие люди не захотят видеть, независимо от прав немногих желающих?

Как общество, мы должны всего лишь осознать, что наше понимание сущности радио и телевидения неверно. Наше сознание десятки лет находилось под влиянием аргумента о том, что радиодиапазона на всех не хватит. Этот аргумент – просто хитрая уловка, навязанная и поддерживаемая искусственно теми общностями, которые получают на этом свою прибыль. Избавившись от ложных образов, телевидение и радио становятся менее похожими на частные земельные участки или морские судоходные трассы и обретают сходство с... книгами.

Обществу придется пройти через период, в который будет формироваться отношение к телевидению как к библиотеке. Ошеломляющее (или даже пугающее) количество литературы – это еще не повод отказываться от личной библиотеки. Чтобы действовать наверняка, необходимо подсчитать возможные (весьма немалые) издержки общества на утилизацию старых телевизоров и создание новых, способных принимать миллионы каналов. Нам уже известен этот путь. Внедрение новой технологии, такой как радио с FM-модуляцией или персональные компьютеры, способно решить проблему «курица или яйцо».

Когда участники рынка улавливают тенденции, мы не всегда удовлетворены результатами их усилий, и дело здесь не в количестве. Если люди предпочтут уверенность в том, что содержимое будет соответствовать нравственным нормам, то рынок предложит каналы с пристойным содержимым вещания и технологии, позволяющие охранять «чистоту». Сложившаяся система существует благодаря мощному финансовому и политическому лобби акул рынка, а также особой любви государства к контролированию прав граждан.

Какой объем государственного контроля необходим?

Определенно, когда заканчиваются слова и начинаются действия, людям требуется защита государства. Доктор Бринкли был лишен лицензии врача; это было правильно тогда и было бы правильно в наше время.

В новом мире свободной беспроводной связи правительство должно выработать меры по совместному использованию диапазона частот. Необходимы технологии, которые будут работать только тогда, когда каждый будет соблюдать нормы мощности и полосы частот. Правительство должно контролировать соответствие производимых устройств нормативам, и мошенники не смогут помешать нормальной связи. Государство также должно разработать и принять стандарты для «интеллектуальных» радиоустройств.

На государство также возложена особая ответственность за оценку научного обоснования мрачных предсказаний власть имущих о рисках внедрения новых технологий – и если обоснования надежны, то государство должно решить, насколько важное влияние на общество окажет блокирование технологических инноваций.

Типичную реакцию радиоиндустрии на новые веяния продемонстрировала осенью 2007 года Национальная ассоциация теле- и радиовещания, развернув рекламную кампанию по блокированию технологии, использующей незадействованные частоты для интернет-связи: «В то время как наши друзья из Intel, Google и Microsoft готовы мириться с системными ошибками, сбоями и обрывами связи, теле- и радиовещатели не могут себе этого позволить».[1] Сугубо научные проблемы интерференции сигналов должны решать ученые, а не рекламщики или конгрессмены. Чтобы рационально и в интересах общества решать подобные вопросы, всегда необходим независимый орган, например, FCC.

И когда все это произойдет, проблема нехватки радиочастот исчезнет. На этом этапе государство может – и по конституции *должно* – перевести свой контроль содержимого информации на уровень газет и книг. Законы о непристойности и клевете будут так же уместны для беспроводных коммуникаций, как и для других источников информации. Здесь Конгресс может принять дополнительные правовые ограничения, возможно, ради национальной безопасности.

Другие методы контроля транслируемых по радиоволнам слов и изображений должны исчезнуть. В спроектированном заново мире информации старая правовая основа неприменима. Есть очень много путей, по которым информация может до нас добраться. Нам необходимо

[1] Алан Фрэнк (Alan Frank), цитируется в «Broadcasters launch ads against device» (Радиовещатели выпускают рекламу против правил), Yahoo! Finance (*biz.yahoo.com*), 10 сентября 2007 года.

взять на себя ответственность за то, что видим мы сами, и за то, что позволено видеть нашим детям. Необходимо научить детей жить в новом мире, изобилующем информацией.

Сегодня нет причин снова вводить «Доктрину равноправия», которая до 1987 года требовала от владельцев станций тратить часть эфирного времени на вещание альтернативных мнений. При достаточном количестве каналов у государства не было бы необходимости регулировать редакторскую деятельность радиокомпаний. Искусственный дефицит частот, по словам судьи Уильяма Дугласа, приводит к тому, что «администрация за администрацией заигрывает с телевидением или радиовещанием, чтобы обслуживать их низменные или псевдоблагие цели».[1] Мнение судьи Франкфуртера о том, что «возможности радио ограничены; они не доступны для всех тех, кто желал бы ими воспользоваться» сегодня является ошибочным.

Биты остаются битами, представляют ли они фильмы, деловые счета, брань или поэзию. Биты остаются битами, передаются ли они движением электронов в медных проводах, световыми пучками в стекловолокне или модулированными радиоволнами. Биты остаются битами, хранятся ли они в гигантских банках данных, на DVD-дисках, пересылаемых по почте, или на flash-картах, выполненных в виде брелока. Контроль свободы слова на радио и телевидении – характерный пример того, как недостатки общества нередко задерживают технический прогресс. Есть и другие примеры, например в телефонии. Законы и нормы, регулирующие информационный оборот, применяются к технологиям, созданным для обмена информацией.

Биты остаются битами, представляют ли они фильмы, деловые счета, брань или поэзию.

Цифровой взрыв свел всю информацию к ее наименьшему общему знаменателю – последовательностям нолей и единиц. Для всех узлов всемирных информационных сетей есть устройства подключения пользователей. Телефонный звонок, личное письмо, телешоу – все это можно получить в едином потоке данных. Биты могут переходить от радиоантенны к оптоволоконному или телефонному коммутатору и снова к радиоантенне множество раз, прежде чем доберутся до вас.

Универсальность битов предоставляет человечеству уникальные возможности. Мы можем выбирать между пересекающимися путями использования информации. К будущему нас ведут базовые принципы,

---

[1] Дело «Columbia Broadcasting System против Национального комитета по демократии», 412 U. S. 94, 154, 29 мая 1973 года.

а не случайности исторического периода. В США цифровая экспансия разрушила многие технологические бастионы, стоящие на пути к реализации Первой поправки. Зная, что информация – это только биты, все общества вплотную подошли к трудным вопросам о том, где информация может быть общедоступной, а где ее следует контролировать или запрещать.

Заключение | После взрыва

Биты, освещающие весь мир

В греческом мифе титан Прометей украл у главного бога Зевса огонь и принес его людям, а вместе с огнем – и многие ремесла. Зевс отомстил, наслав на человечество пороки и болезни. С этих пор люди пытаются выжить, используя все доступные возможности.

Миф о Прометее – это рассказ о технологиях. Технологии, как и огонь, сами по себе ни хороши, ни плохи. Их ценность зависит от нашего умения их применять. Овладев какой-либо технологией, общество изменяется. Этот процесс необратим.

Информационные технологии – это особый «огонь». Биты – это атомы информационных пожаров. С помощью информационных инструментов мы можем делать то, что иначе невозможно. Хорошо ли, плохо ли, но эти технологии позволяют нам мыслить, делать умозаключения, творить, выражать свои чувства, спорить, соглашаться, учиться и учить способами, прежде недоступными. Они соединяют людей в пространстве в пары и группы. Они увеличивают мощь наших голосов и чувствительность наших ушей. Они также усиливают нашу способность запугивать, раздражать и ненавидеть других и искажают их представления о нас. Они предоставляют возможность зарабатывать и тратить деньги, а также красть их, не выходя из дома.

В греческой мифологии Прометей, принесший огонь, столь велик, что в поздних версиях мифа ему приписывается даже создание человечества. Как изменится общество за ближайшие десять-двадцать лет под влиянием невообразимой мощи цифровых технологий?

Разумеется, мы этого не знаем. Но если события будут развиваться в тех же направлениях, что и сегодня, вполне возможно, серьезно изменятся три характерные грани человеческой культуры: осознание индивидуальности и права на частную жизнь, право на свободу слова и творческая, сторона человеческой натуры, от которой зависит прогресс.

Осознание индивидуальности и право на частную жизнь

В начале цифровой экспансии споры о праве на частную жизнь, казалось, переросли в настоящую войну. Граждане хотели защититься от вторжения. Общественные образования – корпорации и государство – хотели извлечь выгоду из информации, которую рядовые граждане желали бы скрыть.

В действительности все было намного сложнее.

Развитие технологий позволило намного легче собирать данные, не привлекая внимания. Многие поддались соблазну, жертвуя правом на частную жизнь – зачастую даже не осознавая, от чего отказываются. Далеко не каждый клиент задумается о том, почему универмаги сохраняют электронные журналы покупок. Даже без дисконтных карт в кассе объединяются данные кредитной карты и штрих-кода, создавая запись об имени покупателя и его предпочтениях, от простейших до самых интимных. Чтобы сохранить право на частную жизнь, приходится отказываться от многих удобств, а большинство людей к этому не готовы.

Первая информационная революция

«В нем зародыш всех революций. Оно является совершенно новым средством выражения человеческой мысли; мышление облекается в новую форму, отбросив старую. Это означает, что тот символический змий, который со времен Адама олицетворял разум, окончательно и бесповоротно сменил кожу» (Виктор Гюго об изобретении книгопечатания, «Собор Парижской Богоматери»).

Следующее поколение, возможно, даже не будет считать, что чем-то жертвует. Как сказал Сократ, «непознанная жизнь не стоит того, чтобы быть прожитой», однако тот, кто вырос среди социальных сетей вроде Gmail или MySpace, может считать жизнь, выставленную напоказ, вполне нормальной. Генеральный директор корпорации Sun Microsystems Скотт МакНили мудро заметил: «У вас в любом случае больше не будет закрытой частной жизни, забудьте об этом».

Просто отказаться от попыток не так-то легко, когда общественные связи проходят через дисплей компьютера. Общаясь, в основном, лицом к лицу или по телефону, мы могли не доверять человеку, заявляющему, что он из банка, и относились спокойно к тем, кого знали (или считали, что знаем). В электронном мире происходит обратное – мы доверяем сайту банка, в котором храним крупные суммы, но нам приходится постоянно держать в уме, что близкие друзья по электронной переписке могут оказаться самозванцами. Где в умах нового поколения проходит

граница между личным и общественным? Нужны ли нам законы о поддельной дружбе?

Когда электронная конфиденциальность теряется в облаке битов и осторожность приходит в социальные сети, какие общественные институты подвергаются угрозе разрушения? Общество, каким мы его знаем, функционирует благодаря сети связей между группами, отвечающими за свои действия. Что будет, если изменится концепция личной индивидуальности? Устоят ли фундаментальные основы личной неприкосновенности и индивидуальности перед цифровым взрывом?

Что мы можем сказать и кто нас услышит?

Цифровая экспансия коренным образом изменяет средства общения людей. Прежние технологии, позволяющие тиражировать тексты, изречения и изображения, тоже в свое время изменили мир – но у каждой из них есть уязвимые места. Вашу книгу могут прочесть миллионы – но только если у вас есть возможность ее опубликовать. Вы можете раскрыть скандальные сведения, которые низвергнут правительство, – но только если поведаете об этом в газете. Вас услышат миллионы – но только если вы вхожи на радиостанцию.

Сегодня желающие рассказать о чем-то всему миру уже не зависят от прихотей владельцев репродукторов и печатных станков. В США кто угодно может сказать что угодно – не спрашивая разрешения у церкви или светских властей – и быть услышанным миллионами. Никто не обязан слушать или читать вас, но довольно легко поместить сообщение в такое место, где содержимое сообщения станет доступно миллионам людей.

Этому есть своя цена. Не исчисляемая деньгами – веб-сайты дешевы, а электронная почта еще дешевле. Плата состоит в том, что говорящий должен полагаться на множество посредников, передающих сообщения, поэтому есть множество способов подслушать, отфильтровать или отредактировать ваши заявления. Уязвимые места усложнились и рассредоточились, но не исчезли. Те же чудеса технологии, которые создали революцию коммуникаций, служат и «Старшему Брату». С каждым годом совершенствуются технологии распознавания речи, и надо готовиться к тому, что вскоре каждое сообщение электронной почты, каждый телефонный звонок, каждое телевизионное шоу будет проходить через машинный эквивалент человека-цензора. Машины будут внимательно наблюдать, не скажет ли кто «лишнее», что бы этим «лишним» ни казалось.

Правительство подслушивает и подсматривает, чтобы защитить национальную безопасность, политическую оппозицию и общественную мораль. Поставщики услуг связи хотят знать, для чего потребители используют коммуникационные сети, чтобы потом ввести новые, наиболее выгодные услуги – такая мягкая форма корпоративной цензу-

Несмотря на невообразимое распространение средств связи в последнюю четверть века, все еще ведется спор, сохранится или нет в будущем та же свобода слова, что и в прошлом.

ры, когда нежелательные коммуникации искусственно замедляются или дорожают. Поставщики информации анализируют запросы потребителей, чтобы установить на нужные узлы сети передачи данных свои рекламные объявления.

Несмотря на невообразимое распространение средств связи в последнюю четверть века, все еще ведется спор, сохранится или нет в будущем та же свобода слова, что и в прошлом, – даже в США, где есть Первая поправка к Конституции. И какой смысл в праве на свободу слова, если тебя никто не слышит – как дерево, упавшее в лесу? Впечатляющий плюрализм наших источников информации угрожает создать общество, в котором никто не учится извлекать рациональные зерна из критики. Слишком просто – решить, кого хочется слушать, а остальных игнорировать. Не ограничит ли в действительности цифровая экспансия получение информации?

Развитие творчества или усиление законных ограничений?

В письме, уже частично процитированном в главе 1, Томас Джефферсон писал: «Тот, кто получает от меня идею, приобретает собственно инструкции, не причиняя мне ущерба; подобным же образом, тот, кто возжигает свою свечу от моей, получает свет, не ввергая меня в темноту». Осветит ли мир цифровой взрыв или, создавая иллюзии, сделает нас слепыми к восприятию истины?

Цифровой взрыв инициировал революцию законов. В прошлом подросткам редко угрожала опасность преследования со стороны федерального уголовного законодательства. В наши дни такие предупреждения о незаконном скачивании музыки и фильмов встречаются повсеместно. В прошлом политическая реклама, включающая несколько секунд дебатов кандидата с оппонентами, не могла навлечь на политика гнев транслирующей компании. Но осенью 2007 года кандидат от республиканской партии Джон МакКейн столкнулся с непониманием со стороны компании Fox News Channel.

Хотите заставить замолчать своих критиков в изменившихся правовых условиях – пригрозите им судом только за то, что критики передают в эфир некогда сказанное вами. Именно так поступил «экстрасенс» Ури Геллер, когда известный скептик Джеймс Рэнди разоблачил фокусы мистика в клипе, выложенном на сервисе YouTube и включавшем восемь секунд выступления Ури Геллера. Даже университеты злоупотребляют законодательством об интеллектуальной собственности, чтобы остановить поток информации. Известное публичное заявление ректора Гарвардского университета (см. рис. 4.3) не могло быть напечатано в этой книге, потому что университет отклонил соответствующий запрос издателя.

Патентное и авторское законодательство в США были разработаны, чтобы стимулировать индивидуальное творчество ради общественного прогресса. Закон нарушил баланс между экономическими мотивами автора и общественным благом, которое несет изобретение. Период времени, в течение которого люди искусства и изобретатели сохраняют исключительные права, был установлен достаточно долгим, чтобы окупить затраты автора, и достаточно коротким, чтобы стимулировать дальнейшее творчество. Есть важный предел прав на интелектуальную собственность, и правовая система в теории не поощряет злоупотребление авторством в ущерб инженерному или творческому прогрессу.

Когда механические инструменты были вытеснены средствами обработки информации и письма, музыка и изобразительное искусство стали цифровыми, правила игры изменились. Стороны, получившие самую сильную защиту, теперь являются ведущими корпорациями в своей области, в отличие от оригинальных авторов или конечных потребителей. Хотя информационные технологии призваны избавить от посредников, эти самые посредники становятся только сильнее.

Правовая защита влиятельных посредников, защищающих свои экономические интересы, усилилась именно в то время, когда новые технологии побудили авторов напрямую взаимодействовать с потребителями.

Напряженная обстановка сложилась в мире инноваций. Меры Евросоюза по противодействию монополизации рынка корпорацией Microsoft порождены тем опасением, что монополия на программное обеспечение заглушит инновационные решения, которые могут предложить другие разработчики, если дать им выжить. Власть теле- и радиоиндустрии исключать конкуренцию в эфире нарушает право на свободу слова и подавляет инженерное творчество. При этом возможности использования радиосвязи ограничиваются, а полезные разработки не допускаются на рынок.

Как Соединенные Штаты пойдут в будущее – путем информационной демократии или информационной олигархии? Кто управляет средствами, которыми мы будем создавать и использовать биты?

Пара битов напоследок

Битовый взрыв освещает весь мир (рис. 9.1). Лучше всего освещены Европа и Северная Америка, но свет проникает почти повсюду. Нет никаких физических ограничений, чтобы остановить цифровую экспансию. Биты – это не нефть или уголь. Биты почти не требуют сырья и лишь немного электричества. Они путешествуют по стекловолокну в невероятных количествах и передаются электромагнитным излучением сквозь пространство на большие и малые расстояния. С помощью видеокамер и компьютеров мы создаем новые биты, и их с каждым годом все больше. Есть темные пятна, например Северная Корея, но ког-

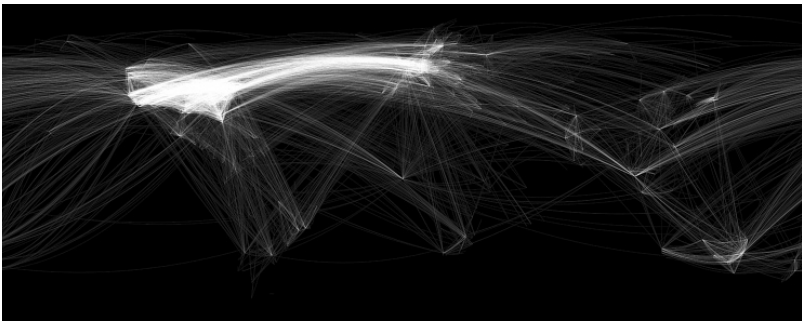


Рис. 9.1. *Подключения к Интернету между маршрутизаторами на карте мира. Сегодня между США и Европой установлено много связей. Если бы вместо количества подключений был показан объем передаваемых данных (заметнее стали бы, например, регионы, где интенсивно используются интернет-кафе), то Африка, Азия и Южная Америка могли бы выглядеть более насыщенно*

Крис Гаррисон, Институт человеко-машинного взаимодействия, университет Карнеги-Меллона, ***www.chrisharrison.net/projects/InternetMap/high/worldBlack.png***

да-нибудь и в эти регионы придет свет. Все факты и мысли, все мельчайшие фотоны света могут быть записаны на диски и сохранены для вечности.

Изобретательность инженеров в обстановке политической и экономической свободы обусловила бурный рост цифровых технологий. Начало этому положил Иоганн Гутенберг, когда изобрел печатный станок. Есть и другие предшественники, в том числе телеграф Сэмюэла Морзе, телефон компании Белл и фонограф Томаса Эдисона. Клод Шеннон стал Прометеем битов – его математические исследования после Второй мировой войны зажгли пламя технологий связи и вычислительной техники, которые в наше время освещают Землю потоками битов.

Битовая экспансия еще не завершена. Мы у нее внутри. Нам неизвестно, к хорошему она приведет или к плохому. Время, когда еще можно решать, кто будет контролировать движение битов, истекает. Биты все еще нечто новое – новый естественный ресурс, предмет раздора регулирующих структур и корпоративных собственников. Жизнь наших потомков будут определять принимаемые нами правовые и экономические решения, которые касаются не самих битов, а скорее того, что от них зависит. Способ, которым биты прояснят или исказят картину мира, определит будущее человечества.

Приложение
Интернет как система и образ мышления

В данном приложении объясняются общие принципы работы Интернета и подводятся некоторые важные итоги его потрясающего успеха.

Интернет как система связи

Интернет – это не просто электронная почта, веб-страницы и цифровые фотографии, как почтовая служба – нечто большее, чем журналы, посылки и письма от вашей тетушки. Интернет не является и просто сетью из проводов и кабелей, как почтовая служба не состоит только из грузовиков и самолетов. Интернет – это система, средство доставки битов независимо от того, что эти биты собой представляют и каким образом они будут доставлены. Чтобы понять причины успешного функционирования Интернета, важно знать принципы его работы и то, почему он служит таким разным целям.

Коммутация пакетов

Предположим, что вы отправляете сообщение электронной почты своему другу Сэму. Сообщение проходит через компьютер, находящийся в Каламазу (Мичиган). Компьютеры, делающие Интернет единой системой, называются *интернет-маршрутизаторами*. Ваш компьютер отправляет электронное письмо; компьютер Сэма его получает. Однако для маршрутизатора пересылаемое сообщение – это просто пакеты битов.

Ваше сообщение скорее всего будет передано по медным проводам, но, вероятно, также проделает некоторый путь по оптоволоконным кабелям. Световоды могут передавать огромные объемы данных на высоких скоростях. Возможно, сообщение будет передано по радиоволнам – например, если передавать его с сотового телефона. Отдельные элементы аппаратной инфраструктуры Интернета принадлежат разным владельцам, в том числе телекоммуникационным компаниям США и правительствам некоторых стран. Интернет функционирует не потому, что

каждая сторона вносит свой вклад в общее дело, а потому, что стороны договорились о способах передачи битов. В соответствии с названием Интернет (Internet, сокращение от interconnecting networks) представляет собой набор стандартов взаимодействия вычислительных сетей. В пределах отдельных сетей могут действовать свои законы, но прием пакетов из Интернета или их отправка в Интернет должны выполняться по общим правилам.

В 1970-х разработчикам Интернета приходилось принимать исключительно важные решения. Одно из них – о размере сообщения. Почтовая служба устанавливает стандарты на размеры и вес посылок. Вы не можете отправить своей тетушке двухтонную посылку, даже если сумеете доставить ее в почтовое отделение. Нужно ли ограничивать размер интернет-пакетов? Предвидя, что в будущем придется пересылать очень большие сообщения, разработчики придумали, как обойти ограничение на размер сообщения.

Второе важное решение касалось самой природы вычислительных сетей. Очевидной представлялась идея сетей с коммутацией каналов, но она была отвергнута. Прежние телефонные сети были полностью коммутируемыми. Чтобы обслужить ваш звонок тетушке, коммутатор должен был соединить провода на всем пути от вас до тетушки в одну электрическую цепь, насколько возможно. Конструкция коммутатора ограничивала количество возможных соединений. Для обслуживания большего числа одновременных соединений требовался коммутатор с большим числом гнезд. Вычислительная сеть с коммутацией каналов обеспечивает надежную связь, однако ее реализация стоит недешево. Большая часть коммутируемого оборудования редко загружена полностью.

Итак, на заре Интернета разработчики должны были решить проблему отправки сообщений неограниченного размера. Также требовалось спроектировать Интернет таким образом, чтобы его пропускная способность была ограничена только количеством передаваемых данных, но не числом подключенных компьютеров. Чтобы выполнить оба условия, инженеры спроектировали сеть с коммутацией пакетов. Единица пересылаемой по Интернету информации называется *пакетом* и имеет размер не больше 1500 байт. Примерно такое же число букв можно уместить на почтовой открытке. Любой блок данных большего размера разбивается на нужное число пакетов, которые соответствующим образом пронумерованы, так что они могут быть снова собраны в единое целое в пункте назначения.

Пакеты, составляющие одно сообщение, могут быть доставлены по разным маршрутам и в разном порядке. Представьте, что почта доставляет только открытки, не больше чем 1500 букв на каждой. Чтобы переслать «Войну и мир», понадобятся тысячи открыток. Можно переслать даже фотографию, если разбить ее на столбцы и строки и указывать на открытках информацию о каждом кусочке (его строку, столбец

и цвет). Получив все открытки, адресат (теоретически) сможет восстановить изображение.

Практическая работоспособность Интернета обеспечивается невероятной суммарной скоростью передачи данных и производительностью конечных компьютеров, которые могут разделять на пакеты и собирать заново сообщения так быстро, что пользователи даже не всегда это замечают.

Ядро и периферия

Условно можно разделить почтовую службу на ядро и периферию: периферию мы видим (это почтовые ящики и почтальоны), а ядро – это то, что обеспечивает работу всей системы. У Интернета тоже есть ядро и периферия. Периферию составляют конечные узлы, непосредственно взаимодействующие с пользователями, например наши с вами компьютеры. Ядро Интернета – это все те связи, которые образуют суперсеть, – собственно Интернет. Ядро включает компьютеры, принадлежащие телекоммуникационным компаниям, которые и отвечают за доставку пакетов.

Интернет-провайдер, или *поставщик услуг Интернета*, – это любой компьютер, который предоставляет доступ в Интернет или выполняет функции, позволяющие различным частям Интернета взаимодействовать. Организация, управляющая работой такого компьютера, тоже обычно называются интернет-провайдером. Ваш провайдер – скорее всего, телефонная или кабельная компания (а если вы живете в сельской местности, то спутниковая компания). Университеты и крупные компании нередко подключаются к Интернету своими силами. «Услугой Интернета» также может быть пересылка информации внутри ядра ближе к пункту назначения. В США множество интернет-провайдеров, и система работает как единое целое, потому что они взаимодействуют друг с другом.

В сущности, Интернет состоит из компьютеров, пересылающих пакеты битов, в которых содержится запрос на услугу, и компьютеров, посылающих ответные пакеты. Могут быть уместны и другие сравнения, но метафора «услуги» довольно близка к истине. К примеру, вы вовсе не «посещаете» веб-страницу интернет-магазина, подобно туристу, привлеченному витриной. Ваш компьютер отправляет веб-серверу магазина особый запрос, а сервер высылает ответ, который может содержать подробное описание того, что вы искали, а также дополнительные предложения, возможно, основанные на ваших предыдущих запросах. Ваши «посещения» оставляют цифровые «следы»!

IP-адресация

Пакеты доставляются по назначению, потому что помечены *IP-адресами*, которые состоят из четырех чисел – от 0 до 255 каждое. (Числа

от 0 до 255 соответствуют всем возможным комбинациям из 8 бит – от 00000000 до 11111111. IP-адрес, таким образом, состоит из 32 бит. IP – сокращение от Internet Protocol, как объясняется ниже.) Типичный IP-адрес выглядит так: 66.82.9.88. Диапазоны IP-адресов присвоены интернет-провайдерам; те, в свою очередь, присваивают IP-адреса отдельным пользователям.

Возможное количество IP-адресов составляет 256 × 256 × 256 × 256 – примерно 4 миллиарда. До миниатюризации, на заре Интернета, такое количество казалось чудовищной расточительностью. Если бы в то время у каждого человека был компьютер, то всем компьютерам могли бы быть присвоены уникальные IP-адреса.

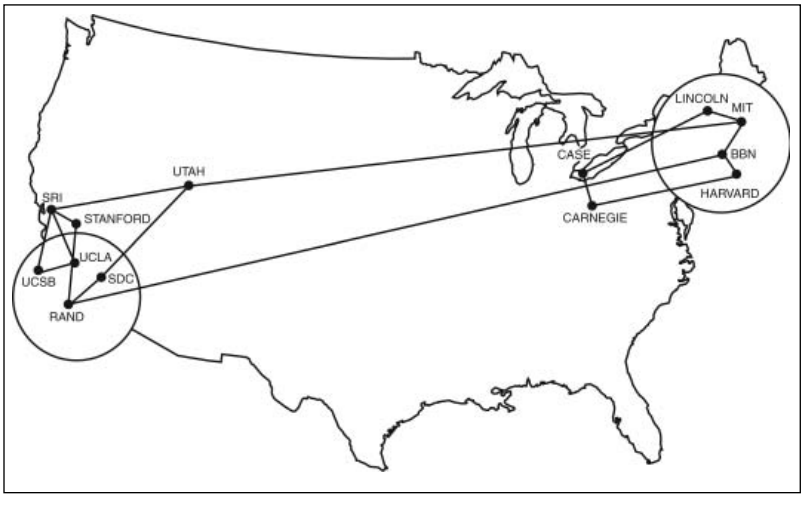


Рис. А.1. 13 первых компьютеров сети ARPANET (из которой позднее вырос Интернет) в декабре 1970 года. Узлы сети были расположены в кампусах Калифорнийского университета в Санта-Барбаре (UCSB на рисунке) и Лос-Анджелесе (UCLA), Стэнфордском исследовательском институте (SRI), Стэнфордском университете (STANFORD), корпорации Systems Development Corporation (SDC), корпорации RAND, Университете штата Юта (UTAH), университете Case Western Reserve (CASE), Университете Карнеги–Меллон (CARNEGIE), лаборатории Линкольна (LINCOLN), Массачусетском технологическом институте (MIT), Гарвардском университете (HARVARD) и корпорации Bolt, Beranek & Newman, Inc (BBN)[1]

[1] Харт Ф., Маккензи Э., Макквиллиан Дж., Уолден Д. (Heart, McKenzie, McQuillian, Walden) ARPANET Completion Report, Bolt, Beranek and Newman (Отчет о завершении реализации сети ARPANET корпорации Bolt, Beranek & Newman, Inc.), Берлингтон (Массачусетс), 4 января 1978 года.

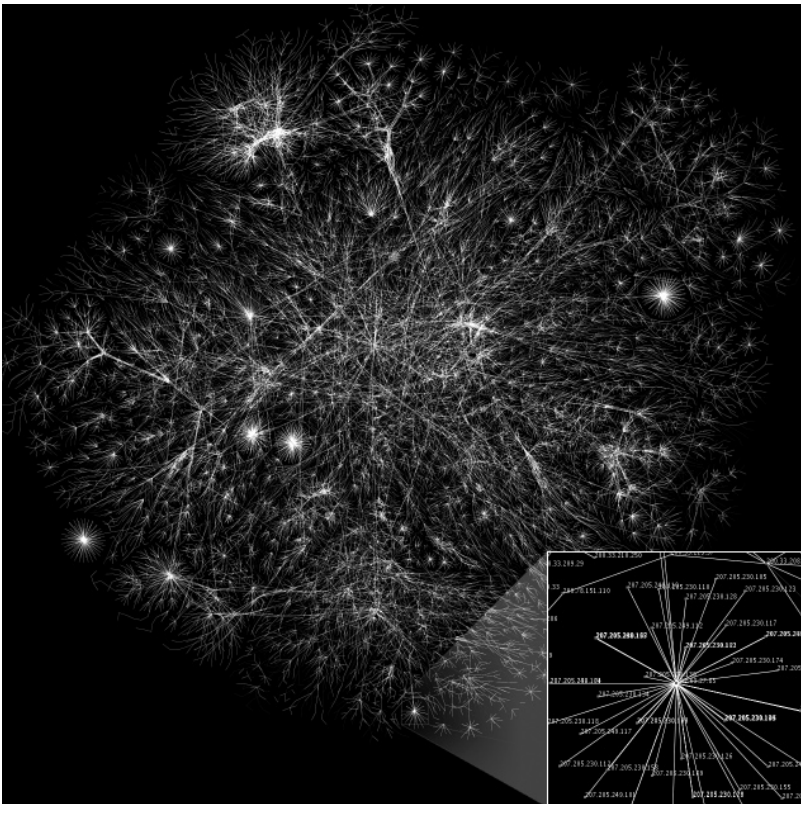


Рис. А.2. *Потоки данных в небольшой области Интернета в настоящее время. Каждый отрезок соединяет два IP-адреса сети. Длина отрезка условно показывает временную задержку сигнала между узлами. Тысячи перекрестных соединений не показаны*

Википедия, http://en.wikipedia.org/wiki/Image: Internet_map_1024.jpg. Файл лицензирован в соответствии с Creative Commons Attribution 2.5 License

На рис. А.1 показаны 13 компьютеров, составлявших единую сеть в 1970 году. В результате миниатюризации электроники появились сотовые телефоны и множество других компактных устройств. Сегодня к Интернету подключены сотни миллионов устройств (рис. А.2) и похоже, что в долгосрочной перспективе возникает недостаток IP-адресов. Уже ведется разработка проекта новой версии протокола IP, в котором предусмотрена адресация длиной в 128 бит. При этом количество возможных IP-адресов выражается числом, состоящим из тройки с 38 нулями. Это примерно в десять миллионов раз превышает количество бактерий на планете.

Важной частью инфраструктуры Интернета являются *серверы доменных имен* (Domain Name Server, DNS). Это компьютеры, предоставляю-

щие информацию о том, каким IP-адресам соответствуют так называемые доменные имена, такие как *harvard.edu*, *verizon.com*, *gmail.com*, *yahoo.fr* (суффикс «fr» это код страны – Франция), *mass.gov*. Когда ваш компьютер отправляет сообщение электронной почты или запрашивает веб-страницу, сначала доменные имена транслируются в IP-адреса, и только после этого пакеты отправляются в ядро Интернета. Не имея представления о доменных именах, маршрутизаторы отправляют пакеты, руководствуясь указанными в них IP-адресами.

Внутренняя сеть предприятия, подключенная к Интернету посредством одного компьютера-шлюза, может использовать единственный IP-адрес. Пакеты при этом снабжаются дополнительной информацией – номером «порта», – так что шлюз может перенаправлять запросы к нужному компьютеру в частной сети. Этот процесс называется *преобразованием сетевых адресов* (Network Address Translation, NAT). Механизм NAT помогает экономить IP-адреса. Также NAT не позволяет внешним компьютерам выяснить, чей компьютер в действительности выполнил запрос, – информация о том, какому компьютеру соответствует каждый порт, хранится только на шлюзе.

IP-адреса и преступность

Медиакорпорации идентифицируют случаи нелегального скачивания звуковых файлов по IP-адресам, на которые эти файлы отправлялись. Но IP-адрес редко является индивидуальной собственностью, поэтому гарантированно установить личность нарушителя нелегко. Интернет-провайдер присваивает IP-адрес компьютеру пользователя лишь на какое-то время. Когда сеанс работы завершается, IP-адрес освобождается и может быть передан другому узлу. Если задействован механизм NAT или один беспроводной маршрутизатор одновременно обслуживает множество пользователей, обычно практически невозможно установить, кому именно был назначен конкретный IP-адрес. Если ваш беспроводной маршрутизатор не обеспечивает безопасность соединения, соседи могут подключиться к нему и создать вам серьезные проблемы, незаконно скачивая файлы.

Ключ ко всему: передача пакетов

Все, чем занимается ядро Интернета, – это передача пакетов. Каждый маршрутизатор связан с несколькими соседними либо с периферией Сети. Получив очередной пакет, маршрутизатор анализирует IP-адрес и решает, на какой ближайший узел переслать этот пакет, руководствуясь своей «картой» известной области Интернета. У маршрутизатора

есть некоторый объем памяти – *буфер* для временного хранения пакетов, которые поступают быстрее, чем могут быть обработаны. Если буфер переполняется, маршрутизатор просто игнорирует поступающие пакеты, предоставляя другим элементам системы смириться с потерей данных, если это допустимо.

Пакеты содержат несколько избыточных битов для проверки на наличие ошибок. Для аналогии предположим, что Алиса из главы 5 хочет подстраховаться от того, чтобы буквы на отправленной ею открытке не были стерты или заменены. Для этого Алиса может добавить к тексту на открытке последовательность из 33 бит, показывающих, что текст на открытке содержит четное или нечетное количество букв А, Б, ..., Я. Боб может проверить состояние текста, подсчитав буквы и проверив четность по 33-битному «отпечатку». В Интернете все маршрутизаторы выполняют подобную проверку и не пересылают поврежденные пакеты.

Формат пакетов данных – какие биты представляют собой IP-адрес и другую служебную информацию, а какие собственно сообщение – определяется протоколом IP (Internet Protocol – протокол Интернета). Все, что передается в Интернете – веб-страницы, сообщения электронной почты, фильмы, сеансы IP-телефонии, – разбивается на пакеты. Как правило, все пакеты обрабатываются одинаковым образом маршрутизаторами или другими устройствами, использующими протокол IP. Протокол IP обеспечивает доставку всех пакетов, насколько это возможно. Маршрутизатор, поддерживающий IP, доставляет пакеты без гарантии, однако во всей сети гарантированная доставка возможна, поскольку все другие протоколы являются надстройками над протоколом IP.

Протоколы

Сетевой *протокол* – это стандарт обмена сообщениями между компьютерами в сети. Термин взят из дипломатии. Дипломатический протокол – это соглашение, способствующее общению двух не доверяющих друг другу сторон. Над этими сторонами нет никакой общей власти, которая могла бы управлять их поведением. Сетевые компьютеры находятся в похожей ситуации взаимного недоверия и одновременно сотрудничества. Нет никого, кто контролировал бы весь Интернет. Любой может стать частью всемирного информационного обмена. Для этого нужно осуществить физическое подключение и следовать общим для всех правилам обмена битами между узлами.

Тот факт, что пакеты могут быть не переправлены, или «отброшены», как сказано в стандарте, наводит на мысль, что, например, отправленное в редакцию письмо может никогда не дойти до адресата. Конечно, сообщение электронной почты может потеряться, но причина этого обычно кроется в персональном компьтере или машине провайдера, но не в ядре Интернета. Для гарантированной доставки (даже если ее не

гарантируют отдельные узлы) периферийные компьютеры используют протокол более высокого уровня. Этот протокол носит название *протокол управления передачей* (Transport Control Protocol, TCP). Обычно упоминается не TCP, а TCP/IP – связка протоколов.

Чтобы понять общий принцип работы протокола TCP, предположим, что Алиса собирается отправить Бобу полный текст книги «Война и мир» на открытках. Открытки пронумерованы, так что Боб при получении может собрать их в нужном порядке, даже если часть открыток задержится. Открытки могут теряться при доставке, поэтому Алиса хранит их копии. Алиса не выбрасывает копию до тех пор, пока Боб не сообщит, что получил открытку. Для этого Боб, получив открытку от Алисы, отправляет ей свою открытку, где указывает номер полученной открытки. Разумеется, открытки Боба тоже могут потеряться, поэтому Алиса записывает, когда и какую открытку она отправила. Если Боб не пришлет подтверждение в течение оговоренного срока, Алиса отправит Бобу копию. Здесь появляется сложность: Боб должен знать, как игнорировать лишние копии. Но все это можно реализовать.

Примерно так же работает протокол TCP, разве что скорость передачи пакетов в Интернете гораздо выше. В результате электронная почта, использующая TCP, обеспечивает надежную доставку: если сообщение доставлено, то оно в точности соответствует отправленному.

TCP – не единственный протокол доставки пакетов, использующий IP. Приложения реального времени, такие как интернет-видео или IP-телефония, не могут ждать повторной передачи потерянных пакетов. Такие приложения просто отправляют пакеты в «свободное плавание», не заботясь о потерях. Протокол, не гарантирующий доставку данных, называется UDP; этот протокол, как и многие другие, передает пакеты протоколу IP для пересылки к месту назначения.

В общих чертах разницу между низкоуровневым и высокоуровневым протоколами можно показать на примере почты. Почту первого класса, приоритетную, макулатурную и экспресс-почту доставляют одни и те же грузовики и самолеты. Загрузка/выгрузка почтовых мешков в транспорт производится в соответствии с низкоуровневым протоколом. Сбор почты в отделении и ее доставка к транспорту, а также доставка почты адресатам после ее выгрузки производятся согласно некоторому набору протоколов высокого уровня, соответствующих заказанной услуге.

Протокол IP не просто основа для множества протоколов более высокого уровня. Важнейшее свойство протокола IP: он не привязан ни к одной аппаратной платформе. IP подходит для проводов, радиоволн, световодов и даже почтовых голубей. Все, что требуется, – это возможность передавать пакеты битов, включая служебную информацию, к устройствам, которые могут выполнять функции маршрутизаторов.

IP посредством почтовых голубей

Вы можете ознакомиться со следующими документами по организации работы Интернета: RFC 1149 «Standard for the Transmission of IP Datagrams on Avian Carriers» (Стандарт передачи IP-дейтаграмм посредством почтовых голубей) и RFC 2549 «IP over Avian Carriers with Quality of Service» (IP посредством почтовых голубей с QoS). Их текст соответствует стандарту документации для Интернета, хотя авторы предупреждают с некоторой долей ехидства, что «это экспериментальный, не рекомендуемый к широкому применению стандарт».

Для представления битов физическими величинами, такими как амплитуда радиосигнала или длительность светового импульса, существуют протоколы еще более низкого уровня. Протокол IP является вдвойне общим: он может принимать пакеты из различных физических сред и передавать эти пакеты различным протоколам более высокого уровня.

Надежность Интернета

Интернет в высшей степени надежен. В нем нет критически уязвимых мест. Если оборвется один кабель или сгорит узловой компьютер, протоколы автоматически переадресуют пакеты, обходя сбойные участки. Когда в 2005 году на Новый Орлеан обрушился ураган «Катрина», интернет-маршрутизаторы переадресовали пакеты, которые должны были передаваться через этот город. Естественно, пакеты, предназначавшиеся городу, доставлены не были.

Несмотря на огромное число резервных линий связи, если достаточно много их оборвано, то отдельные части Интернета могут быть взаимно недоступны. 26 декабря 2006 года землетрясение, произошедшее недалеко от города Хэнчунь (Тайвань) повредило несколько коммуникационных кабелей, проложенных по дну Южно-Китайского моря. Финансовые рынки Азии на несколько дней потеряли возможность реагировать на события, так как передача данных из Тайваня и Гонконга была невозможна или сильно ограничена.

Говорят, что пока ремонтировали кабели, спама в США тоже было гораздо меньше!

Хотя *ядро* Интернета отличается высокой устойчивостью, надежность связи сильно понижают периферийные компьютеры, имеющие только одну точку подключения. Если вы подключены к Интернету посредством телефонной линии, и какой-нибудь грузовик случайно повредит провода, связь будет потеряна. Некоторые крупные компании подключают свои локальные сети к Интернету несколькими способами – это

решение дороже, но оно оправданно, если надежность связи критически важна.

Интернет как образ мышления

Сверхестественный рост популярности Интернета и его превращение из военной и научной разработки в общедоступную замену почты и телефона заставляют соблюдать его основные принципы. Интернет диктует правила коммуникации, свободного общения и всех видов технического дизайна.

Песочные часы

Стандартная электрическая розетка – это универсальный интерфейс между электростанциями и электроприборами. Потребителям не обязательно знать, является ли источником электричества движение воды, энергия Солнца или внутриатомные реакции, – им нужно просто подключить приборы и заняться привычным делом. Одна и та же розетка – источник энергии для тостера, радиоприемника и пылесоса. И новые приборы подойдут к тем же бытовым розеткам – если, конечно, сделаны по стандарту. Поставщик электроэнергии не заботится о том, на что вы расходуете электричество, до тех пор пока вы оплачиваете счета.

Применяя аналогию песочных часов, можно сравнить розетку с перемычкой их колбы. Через розетку электричество перетекает от всего доступного множества источников энергии к бесконечно разнооб-

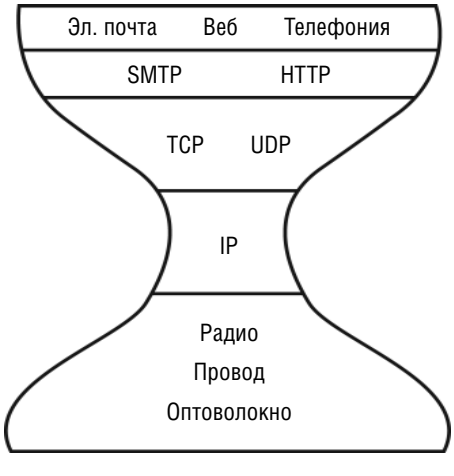


Рис. А.3. *«Песочные часы» (упрощенная схема) протоколов Интернета. Каждый протокол обращается только к соседним сверху или снизу; все данные кодируются в виде IP-пакетов, передаваемых между приложениями и физической средой, составляющей сеть*

разным приборам. Новые изобретения должны лишь соответствовать «перемычке»: электростанция вырабатывает напряжение 220 вольт, и новые приборы должны соответствовать как форме розетки, так и параметрам питания. Представьте, как было бы неудобно, если бы приходилось постоянно подгонять проводку под новую бытовую технику или новые стандарты электроснабжения. Каждый, кто пытался пользоваться одним и тем же электроприбором в США и Великобритании, хорошо знает, что розетки далеко не так универсальны, как интернет-пакеты.

Архитектуру Интернета тоже можно представить в виде песочных часов (рис. А.3) с протоколом IP вместо перемычки. IP определяет форму передаваемых пакетов битов. Множество протоколов высокого уровня используется для самых разных целей.[1] Цитируя отчет, где впервые предложено описание в виде песочных часов, «минимально достаточные элементы <IP> находятся в самой узкой части, а постоянно расширяющийся набор дополнительных средств заполняет верх и низ, показывая, как мало Интернет зависит от провайдеров и пользователей».

Протокол TCP, например, гарантирует надежную доставку, хотя и с возможными задержками, а протокол UDP обеспечивает своевременную, но не гарантированную передачу пакетов. Все высокоуровневые протоколы используют для доставки битов протокол IP. Когда пакеты попадают в «перемычку», они обрабатываются одинаковым образом независимо от протоколов высокого уровня. Уровень TCP и UDP, в свою очередь, передает данные протоколам более высокого уровня, например протоколу HTTP (HyperText Transport Protocol – протокол передачи гипертекста) для обработки веб-страниц или протоколу SMTP (Simple Mail Transport Protocol – простой протокол передачи почты) для отправки сообщений электронной почты. Пользовательские приложения – веб-броузеры, клиенты электронной почты или голосовой связи – расположены на еще более высоком уровне. Они используют протоколы соседнего более низкого уровня, не вникая в их работу.

Ниже уровня IP расположены различные протоколы физического уровня передачи данных. Поскольку универсальный протокол IP находится в «перемычке», приложения (в верней части «часов») могут взаимодействовать с различными физическими каналами связи (в нижней части). Например, когда появились первые беспроводные устройства

[1] Схема Интернета в виде песочных часов была впервые представлена в секции 2 доклада «Realizing the Information Future» (Воплощение информационного будущего) Национальной академии наук, 1994, *www.nap.edu/readingroom/books/rtif/*). Еще один важный доклад, обращающийся к модели песочных часов, – «The Internet's Coming of Age» (Наступление эпохи Интернета) Комитета по положению Интернета в развивающейся информационной инфраструктуре коллегии информатики и телекоммуникаций комиссии естественных наук, математики и приложений Национального исследовательского совета (The National Academies Press, 2001 год), с. 36.

с поддержкой протокола IP (структура Интернета действовала уже давно), ничто из верхней части «часов» не нуждалось в модернизации. Электронная почта, ранее передаваемая по медным проводам, может быть доставлена и посредством радиоволн, таких какие применяются в современных беспроводных маршрутизаторах.

Правительства, медиакомпании, коммуникационные компании иногда хотят, чтобы протокол IP работал иначе, чтобы им было легче фильтровать некоторые виды содержимого, отдавая преимущество другим его видам. Но доводами против таких предложений повторного проектирования Интернета служат универсальность протокола и множество ее неожиданных следствий. Консультант по информационным технологиям Скотт Брэднер писал: «Интернет в сегодняшнем виде сформировался благодаря тому, что вчерашний Интернет не фокусировался на сиюминутных целях. Вместо этого разработчики технологий Интернета и провайдеры ориентировались на гибкость, помогая будущему наступить».[1]

Будущее Интернета: как предотвратить его наступление

Превосходная книга «The Future of The Internet – And How To Stop It» (Будущее Интернета: как предотвратить его наступление) профессора Джонатана Зиттрейна (Jonathan Zittrain) рассказывает об уязвимостях Интернета – быстром росте числа вирусов, атаках на главные серверы – как о следствии открытой структуры и возможности всемирной Сети поддерживать новые разработки. Это то, что профессор Зиттрейн называет «генеративностью» Интернета. Книга показывает, куда может в будущем прийти общество при использовании сети с менее гибкой «приспособляемостью», что позволит избежать нежелательных следствий удивительной податливости Интернета творчеству.

Конечно, целостная социальная структура, в которую развились протоколы Интернета, препятствует засилью частных интересов и включению их любимых функций в инфраструктуру Интернета. Протокол должен быть одобрен Специальной комиссией интернет-разработок (Internet Engineering Task Force, IETF), которая принимает решение на основе простого соглашения, а не голосования. Члены комиссии встречаются лицом к лицу и делятся мнениями, чтобы обосновать свои предложения, поэтому общее мнение комиссии публично, а индивидуальные мне-

[1] «The fallacy of short-term thinking about the Internet» (Ошибочность понимания Интернета в краткосрочной перспективе), *Network World* от 17 октября 2007 года.

ния относительно анонимны, – но ни одно изменение, улучшение или дополнение не может быть принято ограниченной группой лиц.

Главный урок – это важность небольших, тщательно подобранных и открытых стандартов в разработке любой системы, которая получит широкое распространение и будет стимулировать творчество и непредвиденное использование. Являясь простыми соглашениями, стандарты открыты всему новому, если они хорошо подобраны, строго описаны и общеприняты.

Уровни, а не башни

В теории функциональность Интернета может быть обеспечена множеством других способов. Допустим, некая фирма предоставляет исключительно услугу доставки электронной почты в частные дома и учреждения. Фирма должна проложить специальную проводку, одновременно экономичную и удовлетворяющую требованию скорости передачи электронной почты. Фирма должна также приобрести специальные маршрутизаторы, идеальные для маршрутизации электронной почты. В конце концов, фирме необходимо специальное программное обеспечение, идеально приспособленное для работы со специальными маршрутизаторами и специальными проводами.

Другая фирма могла бы заниматься доставкой видео. Передача видеоданных требует более высокой скорости, которая достижима при помощи особых, специализированных маршрутизаторов. Для этого может потребоваться организовать отдельную локальную сеть. Третья фирма может захотеть передавать что-нибудь вроде веб-страниц и попытаться убедить потребителей провести в дома еще и третий вид кабелей.

Огромное преимущество модели «песочных часов» не только в гибкости, обеспечиваемой «перемычкой», но и в логической изолированности верхних уровней от нижних. Разработчики верхнего уровня могут доверять гарантиям умных людей с нижнего, особо не задумываясь, *как* эти самые нижние уровни работают. Правильный способ разработки информационных технологий – уровни, а не множество параллельных вертикальных структур – изолированных башен.

Но мы пока живем в условиях информационной экономики, исторически заключенной в башни посредством права и политики. Есть отдельные правила для телефонии, кабельного вещания и радио. Среда передачи определяет правила. Стоит только взглянуть на названия основных отделов **FCC: отдел беспроводной связи, отдел проводной связи** и так далее.

Но технологии взаимно проникают друг в друга. Телефонные звонки совершаются через Интернет, со всем разнообразием средств передачи. Биты телефонных сеансов ничем не отличаются от битов, составляющих фильмы.

Законы и правила должны соответствовать уровневой организации, а не башенной – этот принцип составляет суть аргументов о регулировании радиовещания, приведенных в главе 8.

Сквозное соединение

Выражение «сквозное соединение» означает, что маршрутизаторы, составляющие ядро сети, должны быть предельно простыми и оптимизированными для выполнения одной-единственной функции – передачи пакетов.[1] Любые более сложные действия должны выполняться мощными компьютерами на периферии сети. Например, протоколы Интернета могут быть разработаны так, чтобы маршрутизаторы проверяли, не было ли потери пакетов. Можно снабдить пакеты информацией, обеспечивающей срочное обслуживание (наподобие экспресс-почты). Можно установить специальные метки для шифрования и дешифрования пакетов на определенных участках маршрута передачи, например при пересечении границ. Но с точки зрения инженера гораздо удобнее оставить ядру сети лишь необходимый минимум функций, возложив более сложные действия на периферию. Один из главных аргументов в пользу последнего – то, что новые приложения могут быть добавлены без необходимости переделки ядра: все специальные функции новых приложений будут выполняться на периферии. Этот подход оказался исключительно успешным, что доказывает огромное число имеющихся сегодня сетевых приложений, о которых первые инженеры Интернета не могли и мечтать.

Тупые сети

Понять философию сквозного соединения можно, осознав, что при мощных периферийных компьютерах Интернета сама по себе сеть может быть «тупой»[2], просто передавая пакеты, которые сами сообщают о своем маршруте. Обратный пример – старая телефонная сеть, где периферийные устройства – это просто «тупые» телефонные аппараты, а качественную связь обеспечивает интеллектуальное коммутационное оборудование, которое само решает, куда следует перенаправить телефонный сигнал.

---

[1] Дж. Х. Зальцер, Д. П. Рид, Д. Д. Кларк (J. H. Saltzer, D. P. Reed, D. D. Clark) «End-to-end arguments in system design» (Причины выбора сквозной реализации при разработке систем), *ACM Transactions on Computer Systems*, 2(4), 277–288 (1984).

[2] Популярное объяснение преимуществ того, что называют «тупыми сетями», можно найти в статье Дэвида С. Айзенберга (David S. Isenberg) «The dawn of the stupid network» (Приход тупых сетей), *ACM Networker* 2.1, февраль/март 1998 года, 24–31, *isen.com/papers/Dawnstupid.html*.

Отделение содержимого от среды передачи данных

Среди явлений XIX века ближе всех к Интернету телеграф. Важнейшим изобретением телеграф считался всего лишь несколько десятков лет. Телеграф способствовал разорению курьерской компании Pony Express, но и сам был вытеснен телефоном. Кроме того, телеграф не получил мгновенного признания: поначалу служба быстрой доставки сообщений не казалась особо ценной.

Одним из первых крупных пользователей телеграфа было агентство Associated Press. Ценны, разумеется, только свежие новости, поэтому для агентства телеграф был очень полезен. Понимая это, служба Associated Press осознала и то, что монопольно распоряжаясь телеграфом, она сможет победить конкурентов. Поэтому агентство заключило особый контракт с монопольным владельцем телеграфной службы Western Union. Контракт предоставлял агентству очень низкий тариф на пользование проводами. Для других новостных агентств на эту среду передачи данных была установлена рыночная цена. В результате агентство Associated Press получило такую власть над распространением новостей, что возникла угроза американской демократии. Агентство могло передавать те политические новости, в которых было заинтересовано, и игнорировать другие новости. Свобода печати существовала в теории, но не на практике, потому что индустрия содержимого контролировала среду передачи данных.

«Викторианский Интернет»

В прекрасной книжечке Тома Стэндейджа (Tom Standage) «The Victorian Internet» говорится о том, что многие социальные явления, порожденные развитием Интернета, наблюдались еще во времена телеграфа. Конфликт владельцев содержимого и средств передачи – единственное новое явление. Не без юмора автор замечает, что телеграф, как и Интернет, использовался для игр на расстоянии почти с самого своего появления.

Современная версия этой игры с моралью – дебаты о «сетевой нейтральности». Владельцы центральных магистралей Интернета получают прибыль от предоставления различных наценок и различных уровней гарантии привилегированным клиентам. Конечно, владельцы могут заметить, что даже почтовая служба лучше обслуживает клиентов, готовых больше платить. А что, если компанию-провайдера купит киностудия, получив независимость от ее цен и сервисной структуры? Вы можете обнаружить, что фильмы дешевле приобрести, чем скачать, да и предоставленные файлы имеют лучшее качество изображения и звука, если произведены родительской компанией-поставщиком содержимого.

Или что будет, если поставщик услуг решит, что какой-то клиент ему просто не нравится, как решила компания Verizon относительно компании Naral? Или провайдер обнаружит, что пользователь применяет сервис непредусмотренным способом? Можно ли в этих условиях обеспечить защиту потребителей?

Еще о свободе информации

Общественная группа SaveTheInternet.com Coalition работает над проблемами сетевой нейтральности и свободы в Интернете. Входящие в нее организации весьма различны по интересам, например Организация владельцев оружия Америки или группа правозащитников в области избирательной и налоговой систем MoveOn.org, Христианская коалиция или группа борьбы за права женщин Feminist Majority. На веб-сайте *SaveTheInternet.com* есть блог и множество ссылок. Блог профессора права Сьюзан Кроуфорд (Susan Crawford) содержит заметки по многим аспектам свободы цифровой информации и ссылки на другие блоги.

Рассмотрим действия интернет-провайдера Comcast в 2007 году.[1] Компания обещала пользователям неограниченный объем передаваемых данных, но затем ограничивала скорость передачи файлов определенных типов.

Инфраструктура компании анализировала пакеты и подменяла те, которые обычно (но не всегда) использовались для передачи файлов видеоданных. Компьютер пользователя, получающий такие пакеты, не распознавал подмену и следовал заложенной инструкции – начать повтор обмена данными с нуля. В результате некоторые сервисы обмена данными без всяких действий со стороны пользователей стали работать очень медленно.

В мире, где существует сетевая нейтральность, такого не могло бы случиться; компания Comcast была бы просто сервисом передачи битовых пакетов без функций срочной передачи или подмены маршрутизируемых пакетов.

В начале 2008 года компания AT&T сообщила, что рассматривала еще более глубокое нарушение сетевой нейтральности: исследование пакетов, проходящих через сети компании, и фильтрацию нелегальной передачи цифровых фильмов и звукозаписей. Примерно как если бы анонсируемое компанией электрическое устройство могло отключить

[1] Питер Свенсон (Peter Svensson) «Comcast blocks some subscriber Internet traffic, AP testing shows» (Тест AP показывает, что Comcast блокирует часть потока данных потребителей), *Associated Press*, 20 октября 2007 года.

питание DVD-проигрывателя, если бы обнаружило, что вы просматриваете пиратскую видеозапись.

Одна компания-поставщик содержимого предположила, что компания AT&T намеревалась извлечь больше прибыли из своего сервиса передачи данных, который использовался бы для соблюдения авторских ограничений. Другими словами, идея, возможно, состояла в том, что люди с большей вероятностью будут покупать лицензионные фильмы у поставщика содержимого AT&T, если поставщик услуг связи (та же AT&T) откажется доставлять пиратские видеофайлы.[1]

Конечно, любая технология, разработанная для контроля передачи нелегальных данных, может быть использована правительством или поставщиками услуг связи для многих других целей. Если поставщики связи могут инспектировать биты, которые вы получаете на персональный компьютер, то эти частные компании могут использовать свои возможности иным способом: чтобы осуществлять слежение, выполнять нужные компаниям законы и навязывать потребителям свою мораль. Просто представьте, что почтовая служба вскрывает вашу почту и решает, какие письма и посылки вы можете получить, а какие – нет!

Открытые интерфейсы

Электрическую розетку можно назвать интерфейсом между электроприбором и сетью питания. Стандартизация интерфейсов способствует развитию техники и повышению эффективности. В мире Интернета интерфейсами являются связи между уровнями протоколов, например, протокол TCP предполагает, что протокол IP выполнит работу по передаче пакетов внутри ядра сети.

При разработке информационных систем всегда есть соблазн создать более сложный интерфейс для какой-то особой цели, например чтобы повысить скорость обмена данными.

Так бывало не раз, однако реализация высокой производительности – совсем не легкое дело. Да и полученные преимущества от высокой скорости не стоят времени, затраченного на разработку и отладку. Закон Мура всегда на стороне более простого решения: подождите немного, и упрощенный проект станет таким же быстрым, как мог бы некогда быть более изощренный.

Еще более важно то, что интерфейсы являются общепринятыми стандартами. Стандарты Интернета принимаются путем удивительного процесса достижения всеобщего согласия, совершенно не иерархичного.

---

[1] «Should AT&T police the Internet?» (Должна ли AT&T выполнять полицейские функции в Интернете?), *CNET News.com*, 17 января 2008, *http://www.news.com/Should-ATT-police-the-Internet/2100-1034-6226523.html?part=dht&tag=nl.e703*.

Стандарты называются RFC – Requests for Comment (предложения для обсуждения). Кто-то размещает предложение, и запускается цикл внесения предложений и проверок, обычно завершающийся созданием чего-то хотя бы полезного, если не признанного всеми совершенным. Все участники знают, что они больше выигрывают, соглашаясь со стандартами и разрабатывая удовлетворяющие стандартам продукты, чем пытаясь действовать в одиночку.

RFC и стандарты

Архив текстов RFC отражает историю Интернета. Архив открыт для всех желающих ознакомиться – просто воспользуйтесь своей любимой поисковой системой. Все стандарты Интернета отражаются в документах RFC, но, как говорит документ RFC 1796, «не все документы RFC являются стандартами».

Алфавитный указатель

Цифры

11 сентября 2001 года
  зачистка информации 154
1984, роман 37, 96

A

Actual Spy, программа 67
Acxiom, компания 57, 74, 77, 79
Adobe Acrobat, 101
Adobe Photoshop 109
ADVISE, проект 77
Amazon, онлайн-магазин 61
analog hole 257
AOL, поисковая система 82
Apple, корпорация 269
Apple iPod, плеер 117
ARPANET, вычислительная сеть 30, 119
ASCII-код 112, 123, 129
AZBilliards.com 34

B

Barnes & Noble, онлайн-магазин 61
bitsbook.com 16
British Entertainment Retailers Association 270

C

C.A.S.P.I.A.N, сообщество 60
CAPPS II, система безопасности 78
captcha 181
CD, формат 117
certification authorities, CA 224
ChoicePoint, сервис 66, 74
Classmates.com 82
Cloud computing, технология 128
CompuServe, поставщик компьютерных услуг 284
cookies 62
Creative Commons, сообщество 272
CSS 214, 261
CSX Railroad, компания 48

D

Department of Homeland Security 76
Digital Millennium Copyright Act, DMCA 257
Digital Theft Deterrence and Copyright Damages Improvement Act 240
Doc, формат 106
Domain Name Server, DNS 365

E

ECHELON, система прослушивания 229
Event data recorder, EDR, 47, 48
Electronic Frontier Foundation, EFF 49
Enron, компания 53
EXIF, формат файлов 43

F

Facebook, сервис 34, 63, 65, 82
Federal Communications Commission, FCC 263, 312
Federal Radio Commission, FRC 323
Flickr 82
flooding 244
FORMAT, команда 130

G

Galeria Kaufhof, торговый центр 46
GIC (Group Insurance Commission) 53
Google 25, 66, 80
  AdWords 176
  Books 156
  Zeitgeist 140
  блокировка в Китае 186
  индексирование книг 274

Google Docs, сервис 128
Google Street View 43
Gopher, программа поиска 147
Government Communication Headquarters, GCHQ 217
GPS 43, 44
Group Insurance Commission, GIC 53

H

HTML 153
HTTP, HyperText Transport Protocol 371

I

IP-адрес 62, 234, 363
iPod, медиапроигрыватель 235
iTunes, сервис продажи музыки 244

L

LiveJournal, сервис 82

M

match.com 34
Microsoft Word
  функция исправления 103
Motion Picture Association of America, MPAA 238
MP3, формат 109, 126
Musicload, сервис продажи музыки 269
MySpace, сервис 34, 62, 65, 82
  обвинение в пособничестве изнасилованию 282

N

Naral Pro-Choice America, компания 22
National Aeronautics and Space Administration, NASA 171
National Weather Service 238
NET Act 239
Network Address Translation, NAT 366
No Electronic Theft Act, NET Act 239
NSFnet, сеть 119

O

Office of Strategic Research and Development, OSRD 148
OnStar, система связи 71
OpenDocument, формат 120, 122
Open source, стандарт 122
optical character recognition, OCR 124

P

PageRank 163
  патент 165
  сервисы отображения 167
pay-per-click 173
PC Pandora, программа 67
PDF, формат 100, 106, 115
PGP, программа шифрования 228
PGP, технология 81
Prodigy, интернет-провайдер 286

R

Recording Industry Association of America, RIAA 232
RFID-метки 44, 46, 58, 79, 94
  и банкноты 64
  ридер 45
  учет покупок 47
robots.txt 152
RootsWeb.com 70

S

Safeway, компания 59, 60, 61
SCO, корпорация 104
sealed storage 254
Sears Holding, компания 91
SMTP, Simple Mail Transport Protocol 371
Snipermail, сервис 57
software-defined radio, SDR 348
Sony, корпорация 247

T

TALON, проект 78
TCP/IP, протоколы 118, 368
The Equatorie of the Planetis 202
TNT, служба доставки 51
Total Information Awareness, TIA 76
trusted boot 254
trusted computing 255
twitter.com 82

U

Ultra High Frequencies, UHF 319
ultra wide band, UWB 346
UNIX
  Berkeley 119
  SCO 104
URL 138

V

VeriSign, центр сертификации 224
Verizon, сотовый оператор 17, 22
Very High Frequencies, VHF 319
VoIP, технология 22

W

Wal-Mart, торговая сеть 29
Web 1.0 82, 138
Web 2.0 82
WEP (Wired Equivalent Privacy, стандарт шифрования 212
WPA (Wi-Fi Protected Access, стандарт 212
WYSIWYG, интерфейс 99

X

Xanga 82

Y

Yahoo! 25, 90
  история 143
YouTube, сервис 82, 94

А

авторские права
  баланс 264, 273
  история развития 237, 265
  первые нарушения 239
  противодействие развитию технологий 256, 260
  противостояние потребителей и владельцев 237
  соучастие в нарушении 243
  судебные иски 233
  ущерб от нарушения 237
Акт об авторских правах 236
Акт о безопасности коммуникаций 67
Акт об удалении сетевых хищников 279
Акт об учете и передаче медицинских данных 91
Акт о добросовестной отчетности по кредитованию 89
Акт о защите авторских прав в цифровую эпоху 257
Акт о защите персональной информации 89
Акт о неприкосновенности информации 66
Акт о праве на неприкосновенность личной жизни 75, 76, 89, 90
Акт о присвоении REAL ID 72
Акт о пристойности в коммуникационных сетях 290
Акт о противодействии электронному воровству 239
Акт о радио 1912 года 319
Акт о свободе распространения информации 76
алгоритм бинарного поиска 157
алгоритм шифрования
  AES 215
  DES 215
  EES 225
  MD5 211
  RSA 222
Альбрехт, Кэтрин 45
Американская ассоциация звукозаписывающих компаний 232
Американская ассоциация кинокомпаний 238
Американский союз гражданских свобод 39
аналоговая точка уязвимости 257
анонимность 38
Антейл, Джордж, композитор 335
Аравозис, Джон 66
Арнольд, Тельма 82
Ассоциация юристов Нью-Йорка 86

Б

базовая станция 17
баннеры 171
Баррет, Дженнифер 77
безопасность интернет-коммуникаций 200
белый список 34
Берман, Джеффри 41
биометрические данные 72
битовая карта 112
биты
  как вид собственности 24
  как документ 99
  определение 17
  тенденции поведения 23
блоги 66
бомбардировка Google 184
Борк, Роберт 61
бракоразводные процессы 59, 67

Браун, Гордон 51
Брин, Дэвид, писатель-фантаст 95
Брин, Сергей, сооснователь Google 166
Бринкли, Джон, врач-шарлатан 326
Брэндис, Луис 85
буфер 367
Буш, Ванневар, исследователь 148
Бэббидж, Чарльз, математик 207

В

Вайтцнер, Дэниел 94
веб-сайты
  архивировные копии 135
Вернам, Гилберт 207
взрыв здания им. Альфреда П. Мурра 295
Виженер, Блез, дипломат 205
военные научные исследования США 148
востановление данных 130
врачебная тайна 56, 68, 91
Всемирная паутина
  как базар битов 141
  начало развития 138
  хаотичность 139

Г

«Гарри Поттер и Дары Смерти» 43
Гейтс, Билл 80
генеалогический веб-сайт 137
Герц, Генрих, физик 316
главный принцип криптографии 211
граница Шеннона 338
Грег, Джадд, сенатор 196

Д

дайджест сообщения 221
данные
  восстановление 130
  миф о восстановлении 132
  необратимое удаление 131
  скрытие 124
  удаление 127
Департамент здравоохранения, образования и социальной поддержки 88
Департамент национальной безопасности 76
Джефферсон, Томас 23
диапазоны частот 315
  классификация 320
  лицензирование 319, 328
  совместное использование 333
дисковые блоки
  индекс 127
  обнуление 129
  определение 127
  пул 129
дисконтные карты 29, 59, 60
Диффи, Уитфилд, криптолог 216
добрые самаритяне 294
доверенная загрузка 254
доверенные вычисления 255

Ж

жучки 71

З

закон Мура 26, 117
  действие 28
законное основание для просмотра записей сотового оператора 18
законодательные акты 89
законодательство по борьбе с отмыванием денег 19
замедление научного прогресса 148
запрос к поисковой системе 139
  на естественном языке 160
  расширенный 158
зашифрованный текст 202
защита детей в Интернете 279, 299

И

идентификационные карты
  в Китае 71
  в США 72
иерархическая организация информации 146
  недостатки 139, 147
интеллектуальная собственность 24
Интернет 362
  как журнальный киоск 300
  как ограниченное пространство 291
  как пиринговая архитектура 243
  клевета 283
  поиск аналогий 281
  порнография 288
  структура 282
  цензура 286, 308
интернет-провайдер 363
интернет-реклама 176

информационная емкость 338
Информационная служба уголовного правосудия 72
Информационный центр электронной конфиденциальности 39, 77
информация
доступность в Интернете 280
управление потоками 281
Иракское досье 105

К

Кадастровая книга Англии 25
цифровая версия 1986 года 133
цифровая версия 2001 года 135
Казиский, Вильям 207
Калипари, Никола, агент итальянской разведки 98, 105
карты местности 34, 68
каталоги интернет-ресурсов 139
Yahoo! 147
Кейт, Фред 92
Келлская книга 111
Керкхоффс, Аугуст, лингвист 213
киберпространство 31
киберсталкинг 302
Китай 70
клиенты 241
Клинтон, Хилари 65
ключ шифра 196
генерация 219
закрытый 218
открытый 218
передача 208
коаны о битах 22
Комиссия по групповому страхованию 53
коммуникационные протоколы 118
IP 118
TCP 118
компьютеры
производительность 25
увеличение производительности 26
конкорданции 157
копирование 24
Корзин, Джон 47
кражи номеров кредитных карт 212
кредитные карты 63, 74, 79
«криптографические войны» 226
кэширование 154
проблема авторских прав 156

Л

Ламарр, Хэди, актриса 335
лицензионные соглашения 91
Лондон
взрывы 37
телекамеры 37, 92

М

Магритт, Рене художник-сюрреалист 107
Майер, Мэган 35
МакИнтайр, Лиз 45
Максвелл, Джеймс Кларк, физик 316
Маркони, Гульельмо, инженер 317
Маркус, Майкл, радиоинженер 343
маршрутизатор 361
мегабайт 117
мегапиксел 112
Мелис, Детлев прокурор ООН 102
Меркль, Ральф, криптолог 216
метаданные 43
определение 104
метапоиск 194
миграция клеветы 32
мобильные телефоны 40, 41, 71, 329
моделирование 108
с чистого листа 109
Мур, Гордон 26

Н

Национальный совет США по научным исследованиям 198
нигерийские письма 122
Никсон, Ричард 75

О

Обама, Барак 65
облачные вычисления 128
обход защиты
дисков DVD 257
публикация сведений 259
форматов данных 253
односторонняя функция 218
оланзапин, препарат 143
побочные эффекты 144
утечка информации 144
опечатанное хранилище 254
оптическое распознавание символов 124
Организация экономического сотрудничества и развития 88

Оруэлл, Джордж 37
ответственность интернет-провайдеров 292, 294, 297, 298
Отдел информационного снабжения 76
открытый текст 202

П

пакет данных 199, 362
парковка 50
Патриотический акт 33, 190
«паук» 153
Пейдж, Ларри, сооснователь Google 166
Первая поправка к Конституции США 86, 287
пиксел 112, 114
пиринговая архитектура 240
  массовые разработки 244
  устойчивость 245
платные автострады 58
повторный вызов 161
Пойндекстер, Джон 76
поисковая оптимизация 182
  мошенничество 183
поисковые запросы 83
поисковые системы 25, 138
  AOL 82
  Overture 172
  Quaero 195
  WebCrawler 171
  Джен 150
  индекс 150
  как использовать 142
  как посредники 141
  качество результатов 163
  контроль информации 140
  локальные 139
  назначение 141
  открытые 194
  представление результатов 142, 168
  принципы работы 149
  специализированные 151
  финансирование 170
  эффект замедления работы Интернета 153
политики безопасности 90
Полная информационная осведомленность, план 76, 77
полоса пропускания 339
Полоцкая, Розалия, эмигрант из СССР 137
порнография 110, 126
ПО с открытым исходным кодом 122
преобразование сетевых адресов 366
принцип Керкхоффса 214
Принципы добросовестного использования информации
  в Европе 92
  в США 88
  перечень 88
прослушивание телефонных разговоров 90
простой протокол передачи почты 371
протокол передачи гипертекста 371
протокол управления передачей 368
пул 129

Р

радиосвязь
  военное применение 335
  законодательное регулирование 319
  изобретение 316
  интеллектуальная 347
  каналы 322
  монополизация рынка 316
  проблемы эксплуатации 317, 322
  современное состояние 314, 320, 330
  цензура вещания 312
  широкополосная 337, 345
разрешение изображения 115
Райдер, Таня 17
ранжирование результатов поиска 163
растровое изображение 112
регион DVD 262
релевантность 160
  подсчет 162
Ривест, Рональд, криптолог 200
Рингли, Дженнифер Кэй 63
Розен, Джеффри 42

С

Салтон, Джеральд, профессор 162
сверхширокополосная связь 346
Сгрена, Джулиана, журналистка 98
Селигманн, Рид 93
семь принципов 90
сетевой протокол 367
сжатие видео 117
сжатие графики 116
сжатие звука 116

система глобального позиционирования 43
Скиннер, Ричард 77
Служба внутренних доходов 75
создание новых устройств 27
соотношение сигнал-шум 341
социальные сети 34, 38, 65, 81
спам 60, 122
  графический 124
  программный фильтр 123
Специальная комиссия интернет-разработок 372
списки избирателей 55
сплетни 85
средства мониторинга действий пользователей 67
средства родительского контроля 67
ссылки
  заблокированные 190
  иерархия 147
  недействительные 152
  рекламные 172
статистический анализ 204
стеганография
  определение 124
  примеры 125
  программное обеспечение 126
Стюарт, Мария, королева Шотландии 204
Суини, Латанья 55

Т

телевизионная реклама 249
теорема Шеннона-Хартли 338
терабайт 151
терроризм 76, 90
тест Миллера 288
технологии
  Cloud computing 128
  Google Docs 128
  видеосжатие 117
  нейтральность 32
  оптическое распознавание символов 124
  от аналоговых к цифровым 109
  смена поколений 117
Томеро, Джон 71
Трисемус, Иоганн 125

У

удаление данных 127, 131
Уоррен, Сэмюэл 85
Управление делами социального страхования 70
управление цифровыми правами 253
Уэллс, Герберт, писатель-фантаст 149
Уэльд, Уильям 55
Уэстин, Алан 86

Ф

файлообменные системы 240
  Napster 240
факторизация 223
Фано, Роберт 86, 96
Федеральная избирательная комиссия 64
Федеральная комиссия по радиосвязи 323
финансовые аферы 29
флудинг 244
Фонд электронной безопасности 39, 49, 293
фоновое выполнение 150
форматирование диска 130
форматы файлов
  DOC 120
  MP3 116
  OpenDocument 120, 122
  PDF 115
  конкуренция 119
  несовместимость 120
  расширения 114
Франкена, Эл 65
Фри, Луи, директор ФБР 199
функция поиска 139

Х

Харири, Рафик, премьер-министр Ливана 102
Хейман, Джозеф 56
Хеллман, Мартин, криптолог 216

Ц

Цезарь, Юлий 201
Центр демократии и технологий 39
центр сертификации 224
Циммерманн, Фил, криптолог 196, 226
цифровая обработка сигналов 109
цифровая подпись 221

цифровое видео 117
цифровое изображение 112
алфавитных символов 123
защита 110
Келлская книга 111
правомерность 110
процесс получения 108
разрешение 115
растровое 112
цифровой сертификат 223
классы 224
цифровые водяной знак 270
цифровые копии 24
цифровые произведения
лицензирование 273
нелегальное копирование 232, 256, 268
новые модели распространения 271
особенности просмотра 251
продажа 252
цифровые следы 41, 49, 52
цифровые фотокамеры 40, 43, 112
процесс съемки 107
разработка 28
ЦРУ 101

Ч

черные кабинеты 212
«черные ходы» в шифрах 197, 225
черный список 34
Четвертая поправка к Конституции США 48
Чосер, Джеффри, средневековый поэт 202

Ш

Шеннон, Клод 21
Шеннон, Клод, математик 208, 338
шифр
абсолютно стойкий 206
Виженера 205
замены 202
методы взлома 210
одноразовый 208
оценка надежности 202, 204, 219
стойкий 205
Цезаря 202
шифрование 52, 80, 196, 201
в XX веке 208
в древности 201
в Средние века 202
защита цифровых прав 253
как оружие 200
коммерческих транзакций 198
правительственный контроль 198
с открытым ключом 201, 216
технология PGP 81
факторы уязвимости 213
шлюз 366
шпионаж в семье 67
Шпитцер, Элиот 19

Э

эксгибиционизм 62
экспоненциальный рост 27
электромагнитное излучение 316
электронная почта 79
бесплатные серверы 81
Этциони, Амитаи 92

По договору между издательством «Символ-Плюс» и Интернет-магазином «Books.Ru – Книги России» единственный легальный способ получения данного файла с книгой ISBN 978-5-93286-162-2, название «Атака битов: твоя жизнь, свобода и благополучие в цифровую эпоху» – покупка в Интернет-магазине «Books.Ru – Книги России». Если Вы получили данный файл каким-либо другим образом, Вы нарушили международное законодательство и законодательство Российской Федерации об охране авторского права. Вам необходимо удалить данный файл, а также сообщить издательству «Символ-Плюс» (piracy@symbol.ru), где именно Вы получили данный файл.