Крис Касперски

bhv®

Техника защиты компакт-дисков от копирования

+ CD-ROM

- Устройство и организация данных на CD-ROM/CD-R/CD-RW
- Программирование приводов SCSI/IDE на высоком и низком уровнях
- Восстановление поврежденных и поцарапанных дисков
- Уязвимости популярных копировщиков Clone CD и Alcohol 120%
- Ошибки в коммерческих программах защиты CD от копирования
- Разработка собственного копировщика CD

МАСТЕР_ПРОГРАММ_

Крис Касперски

Техника защиты компакт-дисков от копирования

Санкт-Петербург

«БХВ-Петербург»

2004

УДК 681.3.06
ББК 32.973
К28

Касперски К.

К28 Техника защиты компакт-дисков от копирования. — СПб.: БХВ-Петербург, 2004. — 464 с.: ил.

ISBN 5-94157-412-6

Рассмотрены устройство и организация данных на дисках CD-ROM/CD-R/CD-RW, секреты профессионального прожига лазерных дисков, а также программирование приводов SCSI/IDE на высоком и низком уровнях. Даны практические советы по восстановлению поврежденных и поцарапанных дисков. Подробно описаны основные механизмы защиты аудиодисков и дисков с данными от копирования и дублирования. Рассмотрены популярные копировщики защищенных дисков (Clone CD, Alcohol 120%) и показано несколько защит, которые предохраняют диски от несанкционированного копирования этими программами. Указаны ошибки, допущенные разработчиками коммерческих пакетов защиты компакт-дисков (StarForce, SecuROM, SafeDisk, Cactus Data Shield, CD-Cops и др.), "благодаря" которым копирование защищенных дисков остается возможным. Показано, как разработать собственный копировщик компакт-дисков.

Для программистов

УДК 681.3.06
ББК 32.973

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. гл. редактора	*Игорь Шишигин*
Зав. редакцией	*Григорий Добин*
Редактор	*Юрий Рожко*
Компьютерная верстка	*Натальи Караваевой*
Корректор	*Виктория Пиотровская*
Дизайн обложки	*Игоря Цырульникова*
Зав. производством	*Николай Тверских*

Лицензия ИД № 02429 от 24.07.00. Подписано в печать 26.08.04.
Формат 70×100 1/16. Печать офсетная. Усл. печ. л. 37,4.
Тираж 3000 экз. Заказ №
"БХВ-Петербург", 190005, Санкт-Петербург, Измайловский пр., 29.

Гигиеническое заключение на продукцию, товар № 77.99.02.953.Д.001537.03.02
от 13.03.2002 г. выдано Департаментом ГСЭН Минздрава России.

Отпечатано с готовых диапозитивов
в ГУП "Типография "Наука"
199034, Санкт-Петербург, 9 линия, 12

ISBN 5-94157-412-6

Содержание

Предисловие

Книга "Техника защиты компакт-дисков от копирования" представляет собой практическое руководство по защите лазерных дисков от несанкционированного копирования, ориентированное на самый широкий спектр читательской аудитории: квалифицированных пользователей, прикладных и системных программистов.

Для создания стойкой, дешевой и надежной защиты вовсе не обязательно иметь дорогостоящее спецоборудование или быть экспертом по безопасности. Обыкновенный бытовой рекордер и пара вечеров свободного времени — вот и все, что для этого надо! Окунитесь в подробное, но вместе с тем увлекательное описание архитектуры лазерных дисков и принципов хранения данных на оптических носителях. Книга, которую вы держите в руках, дает исчерпывающее представление о структуре CD и раскрывает множество секретов, известных только профессионалам высочайшего класса (да и то не всем), излагая материал в доступной форме без высшей математики и практически без ассемблера. И это — ее главная уникальность!

Прочитав эту книгу, вы узнаете: как исказить формат диска так, чтобы он нормально читался (воспроизводился) на подавляющем большинстве приводов CD-ROM, но не копировался бы практически ни одним копировщиком; как привязаться к физической структуре диска так, чтобы копировщики не могли ни воссоздать его, ни сымитировать; какими физико-техническими ограничениями обладают бытовые рекордеры и как использовать это обстоятельство в своих целях.

Вы также научитесь управлять читающими/пишущими приводами на низком уровне, получив максимально полный контроль над лазерным диском, который только позволяет осуществить данная модель привода. При прочих равных условиях диск, защищенный на более высокотехнологичном приводе, не может быть скопирован на всех остальных. Книга подробно рассказывает, чем отличается один привод от другого и на какие его характеристики следует обращать внимание в первую очередь.

В книге подробно рассматриваются, можно даже сказать, разбираются по "косточкам", практически все существующие на сегодняшний день коммерческие защитные пакеты (StarForce, SecuROM, SafeDisk, Cactus Data Shield, CD-Cops и т. д.) с указанием ошибок, допущенных при их реализации, "благодаря" которым копирование защищенных дисков остается все-таки возможным. Защитные механизмы, предлагаемые автором, учитывают горький опыт всех его последователей и не копируются ни одним из существующих на сегодняшний день копировщиков.

Кстати о копировщиках. Здесь вы найдете подробное описание наиболее популярных на сегодняшний день копировщиков защищенных дисков: CloneCD и Alcohol 120%, которые по утверждению их создателей "при правильном сочетании читающего и пишущего приводов могут скопировать любую защиту". Автор убедительно показывает, что это не так, и демонстрирует ряд защит, которые не копируются ни CloneCD, ни Alcohol 120%.

Наконец, книга рассказывает о том, как самостоятельно создать копировщик защищенных дисков, без которого тиражирование защищаемых вами дисков оказалось бы весьма нетривиальной задачей.

Введение

Актуальность защиты лазерных дисков сегодня как никогда велика. Широкое распространение бытовых рекордеров позволило пользователям тиражировать диски чуть ли не в промышленных масштабах, ну или, по крайней мере, львиную долю дисков не покупать, а позаимствовать у приятелей. В то же время многие shareware-программисты распространяют свои продукты на CD-R-дисках по почте, что значительно усложняет задачу хакеров (т. к. если программы нет в открытом доступе, то как ее прикажете ломать?).

В итоге, пользователи интересуются, как ломать защищенные диски, а разработчики — как защитить эти диски так, чтобы их не взломали. Данная книга удовлетворяет интересы обоих групп. Она рассказывает о том, как взламываются практически все, существующие на сегодняшний день, защитные пакеты, и предлагает ряд новых, принципиально не взламываемых защитных механизмов.

Эта книга содержит большое количество уникального, ранее нигде не публиковавшегося материала. Она дает читателю исчерпывающее представление о структуре CD и раскрывает множество секретов, известных только профессионалам, причем материал изложен в доступной форме без вышей математики и практически без ассемблера.

Прочитав эту книгу, читатель научится создавать действительно принципиально некопируемые диски и эта принципиальность будет гарантироваться аппаратными ограничениями современных CD-R/CD-RW-рекордеров. Помимо того, читатель узнает, как избежать конфликтов с нестандартным оборудованием, из-за которых защита отказывается работать у некоторых пользователей или, что еще хуже, приводит к порче их оборудования.

Книга ориентирована на широкой спектр читательской аудитории. По минимуму — никакой специальной подготовки от читателя и не требуется, он даже может не знать, из каких секторов состоит CD-ROM (99% программистов этого, кстати, и не знают). Вся информация, необходимая для осмысленной

работы с CD-ROM, изложена непосредственно в самой книге и отсылки к посторонним источникам минимальны. Читатель не обязательно должен уметь программировать, т. к. все необходимые утилиты для анализа/защиты/взлома лазерных дисков уже прилагаются к книге. Наконец, читатель может воспользоваться автоматическими копировщиками, разработанными автором, которые все сделают за него. Так что книгу стоит покупать уже ради одного содержимого прилагаемого к ней CD.

По максимуму — читатель должен знать математику в объеме вузовской программы, "уметь держать в руках" дизассемблер и "свободно говорить" на Си и ассемблере. Чтение настоящей книги, конечно, не сделает его "богом", но: безграничную власть над лазерными дисками он все-таки получит и сможет вытворять с ними то, что другим и не снилось.

Условные обозначения

Для предотвращения путаницы и одновременно с этим для избежания многословия, в книге вводится ряд условных обозначений, расшифровкой которых мы сейчас и займемся. В частности, условные обозначения CD-приводов:

- **NEC** — _NEC CD-RW NR-9100A; firmware version 1.4;
- **ASUS** — ASUS CD-S500/A; firmware version 1.4;
- **TEAC** — TEAC CD-W552E; firmware version 1.09;
- **PHILIPS** — PHILIPS CDRW2412A; firmware version 1.5.

Кроме того, представлены следующие обозначения копировщиков:

- **Alcohol 120%** — отличный копировщик защищенных дисков, условно-бесплатную версию которого можно получить с сайта **http://www.alcohol-soft.com/**. Автоматически ломает более половины всех существующих типов защит от копирования и позволяет динамически монтировать образы защищенных дисков на виртуальный привод CD-ROM, что очень удобно для экспериментов. К сожалению, монтированию подлежат лишь "правильные" образы, коими большинство защищенных дисков отнюдь не являются.
- **CloneCD** — хороший копировщик защищенных дисков, условно-бесплатную версию которого можно скачать по следующему адресу: **http://www.elby.ch/**. С копированием защищенных дисков в полностью автоматическом режиме CloneCD справляется скорее плохо, чем хорошо, однако после ручного шаманства с настройками и непосредственно самим образом защищенного диска он может скопировать добрую половину существующих типов защит. Утверждение о том, что CloneCD "берет" практически все существующие защиты от копирования — ложное и невероятно далекое от действительности.

Исторический аспект

Первые попытки защиты лазерных дисков датируются началом девяностых годов XX века. Пишущих приводов в то время еще не существовало и в основном приходилось бороться с несанкционированным копированием содержимого CD на жесткий диск. А как же пираты? — спросите вы. Да, действительно, уровень пиратства в России всегда был и остается традиционно велик, но пытаться остановить его программными средствами защиты по меньшей мере наивно. Тот, кто копирует диски в промышленном масштабе, всегда держит при себе пару-тройку опытных хакеров, снимающих такие защиты без труда. Интеллектуальный потенциал "отдела по снятию защит" в пиратских конторах практически неограничен, — здесь работают лучшие из лучших (когда-то, до появления соответствующих законов, автор этой книги в таком "отряде" тоже состоял), и финансовый фактор тут, кстати говоря, вторичен. Платили немного, а "вкалывать" приходилось вовсю, но в этом-то весь интерес и был! Где еще вы могли познакомиться с таким количеством разнообразных защит и приобрести навыки по их ликвидации?

Впрочем, насчет количества я немного загнул. Все многообразие защитных механизмов тех дней сводилось к двум основным типам: LaserLock и кодовое колесо (подробности далее). С появлением пишущих приводов актуальность защит от копирования значительно возросла и они поперли, как грибы после дождя. К началу 2003 года на рынке насчитывалось более полусотни разнообразных методик защиты, большая часть из которых выдавалась за ноу-хау, разработавшей их фирмы. Однако стоило пропустить защиту через дизассемблер, как вас отхватывало щемящее чувство ностальгии по тем далеким и, казалось бы, безвозвратно растворившимся в песке истории временам, когда программное обеспечение поставлялось на дискетах и каждая вторая из них оказывалась защищенной. Современный лазерный диск, конечно, не похож на дискеты десятилетней давности, но методики защиты тех и других по сути своей общие!

В современных защитных механизмах используются следующие методики:

- использование нестандартной разметки;
- внедрение ключевых меток;
- привязка к поверхности;
- "слабые" сектора.

Познакомимся со всем этим семейством поподробнее.

Нестандартная разметка диска в общем случае сводится к умышленному внесению тех или иных искажений, препятствующих нормальной обработке информации. Например, если длину каждого из защищенных файлов искусственно увеличить до ~666 Гбайт, просто скорректировав поле длины, то при попытке копирования таких файлов на винчестер произойдет грандиозный

"облом-с". В то же самое время защита, точно знающая от сих и до сих каждый файл, можно читать, будет работать с ними без особых проблем. Разумеется, такой защитный механизм элементарно взламывается копированием диска на посекторном уровне, однако для этого копировщик должен знать, какое именно количество секторов содержится на диске. Разработчику защиты ничего не стоит исказить служебные структуры диска так, чтобы тот либо представлялся совсем пустым, либо, напротив, разросся до неимоверных размеров. Копировщики, тупо читающие оглавление диска и свято верящие каждому байту служебных данных, просто "заглючат" по полной программе. Те же, кто "поумнее", сумеют определить истинный размер диска по косвенным признакам, двигая оптической головкой до тех пор, пока она еще двигается, а сектора, пролетающие над ней, — читаются. Допустим, защита решит схитрить и в непосредственной близости от конца диска "выроет яму" из множества сбойных секторов. "Ага! — подумают некоторые копировщики, после того как свалятся в нее. — Мы достигли конца!" "А вот и ничего подобного!" — воскликнут другие. Те, что тщательно анализируют чувственную информацию, возвращенную приводом, который-то наверняка знает, в чем причина неудачного чтения — то ли это диск кончился, то ли просто плохой сектор попался.

Другие защиты поступают еще хуже, нагло и самоуверенно записывая оригинальный диск с неустранимыми ошибками (неустанными — значит, не исправляемыми специальными корректирующими кодами, размещенными на CD). Для аудиодисков это означает, что проигрывание последнего будет сопровождаться ожесточенными щелчками. Точнее, должно было бы сопровождаться, но на практике этого не происходит, поскольку разработчики аудиопроигрывателей предусмотрели специальный фильтр, отбрасывающий заведомо искаженные данные и при необходимости прибегающий к *интерполяции* (когда текущая точка отсчета строится на основе усредненных значений предыдущей и последующей точек). Разумеется, это несколько ухудшает качество воспроизведения, но медиамагнатам на это наплевать, да и ухудшение это не такое уж и значительное. С цифровым воспроизведением все обстоит иначе. Ранние версии Стандарта предписывали приводу сообщать лишь о факте возникновения одной или нескольких неустранимых ошибок, но не предусматривали никаких механизмов "маркировки" сбойных байт. Ну считал привод 2352 байта данных, ну убедился, что добрая сотня из них искажена. Что ему дальше-то делать? Интерполировать? Кого и с чем?! Вручную анализировать сигнал и искать "выхлесты"? Слишком сложно, да и качество "восстановленного" звука будет все равно не то. Можно, правда, отважиться "сграбить" аудиопоток с цифрового аудиовыхода, но подавляющее большинство дешевых звуковых карт его не поддерживает, а если и поддерживает, то так "криво", что лучше бы этого вообще не делали. Короче, над хакерами начали сгущаться мрачные тучи без следов присутствия лучика солнца. Но все изменилось, когда производители "выбросили" на рынок приводы, умеющие не только тупо сигнализировать об ошибке чтения,

но и сообщающие позицию сбойных байт в секторе (прямо как в анекдоте: "ты не мудри, ты пальцем покажи!"). Теперь полноценная интерполяция стала возможна и на интерфейсном уровне! Немедленно появились и программы-грабители, использующие новые возможности.

Впрочем, мы сильно забежали вперед. В плане возвращения к анналам перенесемся в те далекие времена, когда никаких оптических приводов еще и в проекте не существовало и все программное обеспечение распространялось исключительно на дискетах, стремительно утекающих как "налево", так и "направо" (собственно говоря, "copyright" именно так и переводится: "скопировано правильно"). Тогда все кому не лень активно "царапали" дискеты всеми подручными предметами: кто побогаче — прожигал магнитное покрытие лазером, кто победнее — орудовал ржавым гвоздем. Защите оставалось лишь проверить присутствие дефекта поверхности в строго определенном месте. Скопировать такой диск без спецоборудования было практически нереально, т. к. даже Левша не смог бы перенести царапины оригинального диска на то же самое место. Правда, хакеры, знающие порты контроллера как свои пять пальцев, быстро сообразили, что если исказить контрольную сумму ключевых секторов, то, несмотря на физическую целостность поверхности, диск будет читаться с ошибкой! Так вот, лазерные диски защищаются тем же самым способом! И абсолютно тем же самым способом они "ломаются"! Производитель может "нафаршировать" диск сбойными секторами, словно рождественского гуся, и при каждом запуске защищенного программного обеспечения проверять их присутствие. Это порождает следующие проблемы: во-первых, далеко не всякий копировщик согласится копировать дефективный диск, а если даже и согласится, то ждать завершения процесса копирования придется ну очень долго (все мы знаем, с какой скоростью читаются дефективные сектора). Но полученная копия окажется все равно неработоспособной, поскольку на ней-то заданных дефектов уже не окажется — а это во-вторых.

Бездумные хакеры просто искажают контрольную сумму сектора, заставляя привод возвращать ошибку (естественно, пишущий привод должен позволять записать сектора с ошибкой контрольной суммы, на что согласится далеко не каждый). Однако это не решает проблемы — ведь "гнутый" сектор читается мгновенно и защита, если она не совсем дура, может сообразить, что здесь, что-то не так! Или, как вариант, она может провести длинное чтение сектора, и тогда сектор с искаженной контрольной суммой начнет читаться!

Как поступают умные хакеры? Ну, это так сразу и не объяснишь. Упрощенно говоря, формат лазерного диска таков, что высокочастотный сигнал, возникающий при чтении последовательности *питов* (pits) и *лендов* (lands), пролетающих над оптической головкой, не имеет опорного уровня, и чтобы привод мог определить, где здесь минус, а где плюс, количество лендов должно быть приблизительно равно количеству питов. О питах и лендах см. далее *главу 1.* Если какой-то участок сектора будет содержать одни питы,

то он окажется катастрофически темным и автоматический усилитель сигнала привода попытается увеличить мощность лазерного луча, ошибочно полагая, что с диском или оптикой не все в порядке. Но ведь тогда часть питов превратится в ленды и привод "обломается" по всем статьям. Сначала он свалится в рекалибровку, поерзает оптической головкой и лишь затем печально констатирует тот факт, что данный сектор не читается. С точки зрения защиты такой сектор будет выглядеть как глубоко дефектный, хотя на физическом уровне поверхность носителя останется и не повреждена.

Теперь самое главное: поскольку привод должен уметь записывать любые мыслимые и немыслимые данные, для преодоления подобных неблагоприятных ситуаций, разработчики были вынуждены предусмотреть специальный механизм их обхода. Существует несколько возможных способов кодирования записываемых на диск данных и привод должен выбрать наиболее благоприятные из них. К счастью (или несчастью), не все приводы столь щепетильны. И поскольку вероятность непредумышленного возникновения неблагоприятных последовательностей исчезающе мала, некоторые (между прочим, достаточно многие) приводы кодируют данные одним-единственным наперед заданным способом. А значит, существует возможность сымитировать сбойные сектора, практически ничем не отличающиеся от настоящих.

Ага! Сказали разработчики защит! Да это же целый клад! Смотрите — если подобрать специальную неблагоприятную последовательность байт, то для ее корректной записи подойдет далеко не всякий привод! При копировании такого диска на обычном приводе оригинал будет изумительно читаться, но копия обнаружит большое количество "бэдов", и скопированный диск запускаться ни за что не будет. Сектора с неблагоприятными последовательностями получили название *"слабых"* (weak), и для их копирования необходимы весьма высокотехнологичные и "навороченные" приводы от "крутых" брэнд-неймов (brand-name). А если такого привода у нас нет и он нам не по карману, тогда что — "кранты", да? А вот и нет! Если только защита не делает дополнительных поползновений, копировщик может рассчитать корректирующие коды для истинной неблагоприятной последовательности, а затем слегка выправить ее и записать на диск. На физическом уровне такой сектор будет читаться без каких-либо проблем, ну а на логическом — привод самостоятельно восстановит его по избыточным кодам в нормальный вид. Правда, если защита прочитает сектор в сыром виде, то она сразу же распознает подлог, так что таким способом копируются далеко не все диски.

Чтобы понять суть следующего защитного механизма, нам тоже придется обратиться к дискетам. Как известно, поверхность дискеты физическим образом делится на концентрические кольца, именуемые *дорожками*, а дорожки в свою очередь делятся на *сектора*. При перемещении головки от последнего сектора одной дорожки к первому сектору следующей дорожки, в силу вращения дискеты мотором, этот сектор успевает "пролететь", и дисководу приходится ждать целый оборот, чтобы дождаться "свидания".

Парни, денно и нощно сидевшие в насквозь прокуренных вычислительных центрах, уже тогда додумались, что если провернуть сектора каждой последующей дорожки, а в случае с винчестером — *цилиндра*, на некоторое расстояние, то скорость последовательного чтения секторов существенно возрастет, поскольку теперь нужный сектор сразу же окажется под головкой. С другой стороны, проворачивая сектора различных цилиндров на различный угол, мы добьемся определенных колебаний скорости обмена, по которым оригинальный диск может быть легко отличен от копии, таких колебаний не содержащей.

Теперь перейдем к лазерным дискам. Никаких цилиндров здесь и в помине нет и последовательность секторов скручена в тугую спираль. Позиционирование на сектора соседних витков дорожки осуществляется путем отклонения лазерной головки магнитной системой (т. е. происходит практически мгновенно), а позиционирование на удаленные сектора вовлекает в движение механизм перемещения головки по специальным "ползункам" — что требует значительного времени. Зная скорость вращения диска и измерив время позиционирования на сектора соседних витков дорожки, мы сможем найти угол между ним, напрямую зависящий от степени закрутки спирали. Различные партии CD-R/CD-RW-дисков обладают различной структурой спирали, и, что самое неприятное, эта структура закладывается непосредственно самим производителем — т. е. диски поступают в продажу с предварительно выполненной разметкой, необходимой для ориентации записывающего привода на "местности". Скопировать защищенный таким образом диск нереально, и приходится прибегать к его эмуляции. Копировщик должен тщательно измерять углы между различными секторами и воссоздать исходную структуру спирали. Процесс сканирования диска занимает чудовищное количество времени (порой несколько суток), но результат того стоит.

Диск также может иметь катастрофически нестандартный формат, — например сектора переменной длины, в результате чего одни из них будут читаться быстрее, другие медленнее. Поскольку всякое изменение длины секторов немедленно отражается на структуре спиральной дорожки, копировщику приходится иметь дело с двумя неизвестными — неизвестным углом спиральной закрутки и неизвестной длиной секторов. С математической точки зрения это уравнение имеет множество возможных решений, но только одно из них правильное. Копировщик может (и должен!) представить несколько вариантов копий, чтобы мы могли самостоятельно решить, какая из них "ломает" защиту, а какая нет. К сожалению, ни один из всех известных мне копировщиков этого не делает.

Впрочем, длинные сектора представляют собой вполне самостоятельную сущность, и некоторые диски используют для своей защиты только их одних. Плохо то, что ни один из всех представленных на рынке пишущих приводов не позволяет управлять длиной записываемых секторов по нашему усмотрению. Правда, одна зацепка все же есть — пусть мы не можем увеличить

длину сектора, но мы в состоянии создать два сектора с идентичными заголовками — привод, успешно прочитав первый из двух секторов, второй просто проигнорирует, тем не менее, видимая длина сектора возрастет вдвое. Минус этой технологии состоит в том, что мы можем увеличить длину секторов лишь на величину, кратную двум, да и то не на всех приводах. Некоторые из них писать спаренные сектора (они, кстати, называются *twin-sectors*) просто отказываются.

Теперь перейдем к ключевым меткам. Помимо пользовательской области сектора, которую исправно копируют практически все копировщики, на лазерных дисках существует множество мест, на которые "не ступала нога человека". Прежде всего это *каналы подкода.* Всего их восемь. Один хранит сервоинформацию, по которой лазерная головка "ориентируется на местности", другой — информацию о паузах, остальные шесть каналов свободны и нормальные копировщики их не копируют, да и не всякие пишущие приводы дают возможность их записывать. Вот сюда ключевые метки защиты и внедряют!

Кстати говоря, каналы подкода хранятся независимо от канала основных данных, и прямого соответствия между ними нет. При чтении канала подхода сектора X, привод может вернуть субканальные данные любого из соседних секторов по своему усмотрению — это раз. А теперь два — большинство приводов обладает крайне плохим постоянством, и при последовательном чтении субканальных данных секторов X, Y и Z нам могут возвратиться, например, данные X, X, X, или Y, Z, X, или Y, Z, Z, или любая другая комбинация последних. Допустим, канал подкода одного из секторов содержит ключевую метку. Допустим, мы пытаемся ее прочитать. Но прочитаем ли? А вот это как раз и не факт! Если сервоинформация окажется слегка искажена, мы вообще не сможем разобраться, субканальные данные каких именно секторов мы прочитали и входит ли наш сектор в их перечень или нет. Единственный выход — воспользоваться качественным читающим приводом, обладающим хорошим постоянством чтения субканальных данных.

И последнее. Записываемые и перезаписываемые диски по ряду характеристик значительно отличаются от штампованных CD-ROM. ATIP[1] представлять, думаю, нет необходимости? Еще существует такая вещь, как TDB (Track Descriptor Block — блок описания трека), среди прочей информации сообщающий мощность лазера и иже с ней. На CD-ROM-дисках ничего подобного, разумеется, нет. Непосредственно подделать природу CD-ROM-диска невозможно, но существует множество утилит, перехватывающих все обращения к приводу и возвращающих то, что нужно, а не то, что есть на самом деле.

На этом нашу краткую экскурсию "по зоопарку защитных механизмов" можно считать законченным. Затем, по мере углубления в книгу, каждый из этих экспонатов будет рассмотрен во всех подробностях.

---

[1] ATIP (Absolute Time In Pre-Groove) — информация о реальном производителе CD-R/RW-носителя, максимальной разрешенной скорости записи и максимальной емкости диска. — *Ред.*

...обход защиты от копирования совсем не то же самое, что нарушение авторских прав! Законы многих стран (в том числе и Российской Федерации) явным образом разрешают создание резервных копий лицензионного носителя. В то же самое время, нет такого закона, который бы запрещал "взлом" легально приобретенного экземпляра программы. Лицензионное соглашение вправе запрещать что угодно, однако статуса закона оно не имеет. Нарушая лицензионное соглашение, вы автоматически разрываете договор с продавцом программы, а значит, лишаетесь всех обещанных им льгот и гарантий. Приблизительно то же самое происходит, когда вы путем замыкания таких-то ножек процессора разблокируете его тактовую частоту. Посадить вас не посадят, но и сожженный процессор (если он вдруг сгорит) вам не обменяют. С другой стороны, распространение взломанных программ уже попадает под статью, и потому лучше не рисковать.

Мысли о хакерах, защитах и программировании

Взломщики и защитники информации не только враги, но и коллеги. Если предположить, что хакеры паразитируют на программистах (пользуясь их неумением строить по-настоящему качественные защитные механизмы), то тогда с неизбежностью придется признать, что программисты паразитируют на пользователях, пользуясь их неумением программировать!

Хакерство и программирование действительно очень тесно переплетены. Создание качественных и надежных защитных механизмов требует навыков низкоуровневой работы с операционной системой, драйверами и оборудованием; знаний архитектуры современных процессоров и учета особенностей кодогенерации конкретных компиляторов, помноженных на "биологию" используемых библиотек. На этом уровне программирования грань между собственно самим программированием и хакерством становится настолько зыбкой и неустойчивой, что я не рисковал бы ее провести.

Начнем с того, что всякая защита, равно как и любой другой компонент программного обеспечения, требует тщательного и всестороннего тестирования на предмет выяснения ее работоспособности. Под "работоспособностью" в данном контексте понимается способность защиты противостоять квалифицированным пользователям, вооруженным хакерским арсеналом (копировщиками защищенных дисков, эмуляторами виртуальных приводов, оконными шпионами и шпионами сообщений, файловыми мониторами и мониторами реестра). Качество защиты определяется отнюдь не ее стойкостью, но *соотношением* трудоемкости реализации защиты к трудоемкости ее взлома. В конечном счете, взломать можно любую защиту — это только вопрос времени, денег, квалификации взломщика и усилий, но грамотно реализованная защита не должна оставлять легких путей для своего взлома.

Конкретный пример. Защита, привязывающая к сбойным секторам (которые действительно уникальны для каждого носителя), бесполезна, если не способна распознать их грубую эмуляцию некорректно заполненными полями EDC/ECC[2]. Еще более конкретный пример. Привязка к геометрии спиральной дорожки лазерного диска, даже будучи реализованной без ошибок, обходится путем создания виртуального CD-ROM-привода, имитирующего все особенности структуры оригинального диска. Для этого даже не нужно быть хакером, — достаточно запустить копировщик Alcohol 120%, ломающий такие защиты автоматически.

Ошибки проектирования защитных механизмов очень дорого обходятся их разработчикам, но гарантированно застраховаться от подобных просчетов невозможно. Попытка применения "научных" подходов к защите программного обеспечения — чистейшей воды фарс и бессмыслица. Хакеры смеются над академическими разработками в стиле "расчет траектории сферического коня в вакууме", и практически любая такая защита "снимается" за 15 минут без напряжения извилин. Вот грубый, но наглядный пример. Проектирование оборонной системы военной крепости без учета существования летательных средств позволяет захватить эту самую крепость чуть ли не на простом "кукурузнике" (MS WDB — "кукурузник"), не говоря уже об "истребителях" (отладчик Soft-Ice — "истребитель", а дизассемблер IDA Pro — еще и "бомбардировщик").

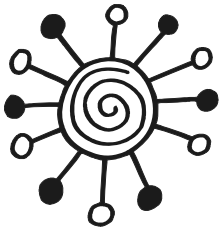
Для разработки защитных механизмов следует иметь хотя бы общее представление о методах работы и техническом арсенале противника, а еще лучше — владеть этим арсеналом не хуже противника (то есть владеть им в совершенстве). Наличие боевого опыта (реально взломанных программ) очень и очень желательно, — пребывание в "шкуре" взломщика позволяет досконально изучить тактику и стратегию наступательной стороны, давая тем самым возможность оптимальным образом сбалансировать оборону. Попросту говоря, определить и усилить направления наиболее вероятного вторжения хакеров, сосредоточив здесь максимум своих интеллектуальных сил. А это значит, что разработчик защиты должен глубоко проникнуться психологией хакеров, настолько глубоко, чтобы начать мыслить, как хакер.

Таким образом, владение технологией защиты информации предполагает владение технологией взлома. Не зная того, как ломаются защиты, не зная их слабых сторон, не зная арсенала хакеров — невозможно создать стойкую, дешевую и, главное, простую в реализации защиту. Книги, рассматривающие вопросы безопасности исключительно со стороны защиты, грешат тем же, что и конструкторы запоминающих устройств, работающих только на запись, — ни то, ни другое не имеет никакого практического применения.

---

[2] EDC/ECC (Error Detection Code/Error Correction Code — коды обнаружения и исправления ошибок. — *Ред.*

[3] MS WDB — это Microsoft Windows Debugger.



Часть I

АНАТОМИЯ ЛАЗЕРНОГО ДИСКА

Глава 1

Организация CD

В этой, преимущественно теоретической, главе читатель знакомится с организацией CD и принципами оптической записи, без знания которых осмысленная работа с защитными механизмами попросту невозможна.

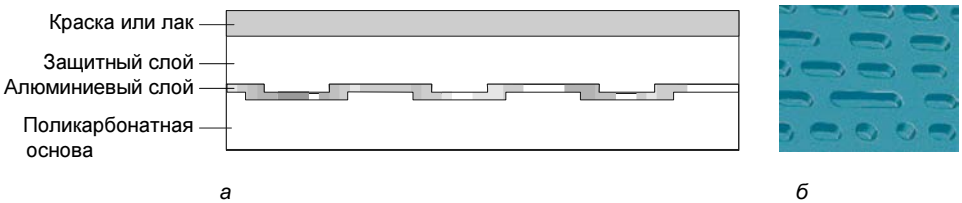


Рис. 1.1. Лазерный диск в разрезе (*а*) и увеличенные питы (*б*)

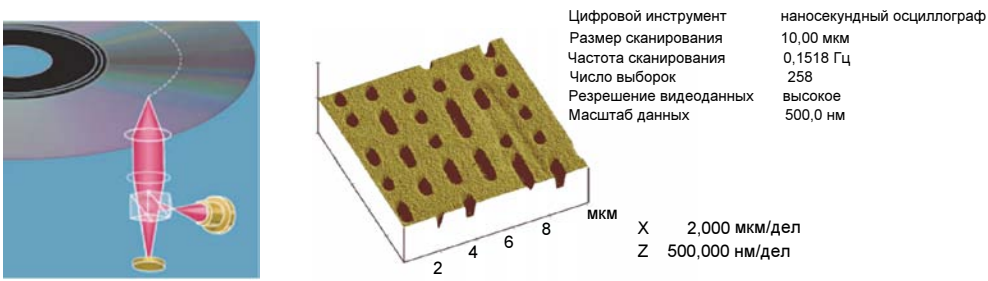


Рис. 1.2. Лазерный диск это все равно что грампластинка

Физически лазерный диск представляет собой пластинку из поликарбоната с нанесенным поверх нее *отражающим* алюминиевым (реже — золотым) *слоем*, защищенным от механических повреждений специальным *защитным слоем* (рис. 1.1). Отражающий слой содержит в себе цепочку углублений или

иначе *питов* (*pits*) и возвышенностей, иначе *лендов* (*lands*), свернутую в спираль, — примерно такую же, как на грампластинке (рис. 1.2), но намотанную в обратном порядке: от центра диска к его краям (фактически лазерный диск является устройством последовательного доступа с ускоренной перемоткой).

Кратко о питах, лендах, EFM-словах, фреймовых кадрах и секторах

Вопреки распространенному заблуждению питы (pits) и ленды (lands) отнюдь не соответствуют двоичному нулю и единице непосредственно. Кодирование информации на CD устроено значительно хитрее и умнее! *Единица представляется переходом от пита к ленду или наоборот, а ноль — отсутствием переходов на данном промежутке* (рис. 1.3). Причем между двумя соседними единицами должно быть расположено не мене двух, но и не более десяти нулей. Ограничение снизу обусловлено технологическими трудностями штамповки, а ограничение сверху — нестабильностью скорости вращения диска. Действительно, пусть стабильность вращения составляет 3%, тогда при считывании последовательности из десяти нулей мы получаем погрешность /3 пита/ленда, что не вызывает никаких проблем. Но уже при чтении пятнадцати нулей погрешность возрастает до половины пита/ленда и приводу остается лишь гадать: в большую или меньшую строну ее следует округлять.

Четырнадцать бит образуют *EFM-слово*, которое по специальной таблице перекодируется в "нормальный" 8-битный байт (собственно ***EFM*** так и расшифровывается: ***E****ight to* ***F****ourteen* ***M****odulation — модуляция восемь на четырнадцать*). Между двумя EFM-словами располагаются три *объединяющих бита* (merging bits), которые, во-первых, служат для разрешения конфликтных ситуаций кодирования (например, за одним EMF-словом, оканчивающимся на единицу, следует другое EFM-слово, начинающееся с единицы), а во-вторых, препятствуют появлению ложных *синхрогрупп* (о чем будет рассказано позже).

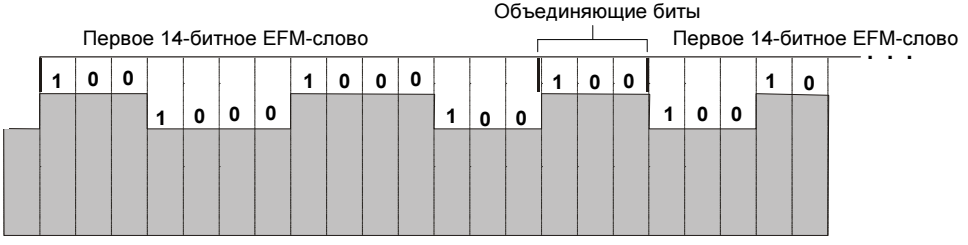


Рис. 1.3. Принцип записи на CD

Группа из 36 байт образует *фреймовый кадр* (*F1 frame*) (рис. 1.4), который состоит из предшествующей ему *синхрогруппы*, байта *субкода* и двух 12-байтных групп *данных*, снабженных 4-байтными полями *контрольных сумм* (или сокращенно CRC — Cyclical Redundancy Check — контроль с помощью циклического избыточного кода).

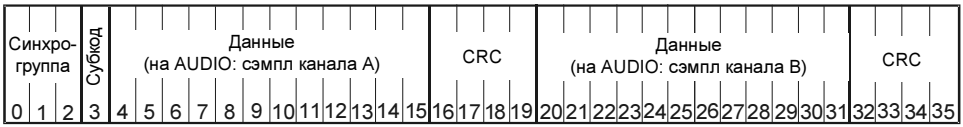


Рис. 1.4. Устройство фреймового кадра

Кадры объединяются в *сектора*, также называемые *блоками*. Каждый сектор состоит из 98 хаотично перемешанных кадров (перемешивание позволяет уменьшить влияние дефектов носителя, поскольку полезная информация как бы "размазывается" вдоль дорожки), причем первые 16-байт всякого сектора занимает специальный *заголовок* (*header*), состоящий из: 12-байтного *поля синхронизации*, 3-байтного *поля адреса* и 1-байтного *поля режима* (рис. 1.5).

Рис. 1.5. Устройство заголовка сектора

Значимость сектора заключается в том, что это наименьший раздел диска, который CD-привод может считать в "сыром" виде. Причем эта "сырость" на ощупь довольно суха. Никакие приводы не позволяют получить содержимое данных кадра как они есть, а принудительно восстанавливают их на аппаратном уровне, используя для этой цели четырехбайтовые поля CRC. Заметим, что отсутствие доступа к действительно "сырым" байтам приводит к невозможности получения побитовой копии диска, а значит, у защитного механизма существует принципиальная возможность отличить, где дубликат, а где оригинал!

Каналы подкода

Среди прочей служебный информации во фреймовый кадр входит один байт *субкода* (*sub-channel byte*), также иногда называемый *байтом субканала* или *управляющим байтом* (рис. 1.6).

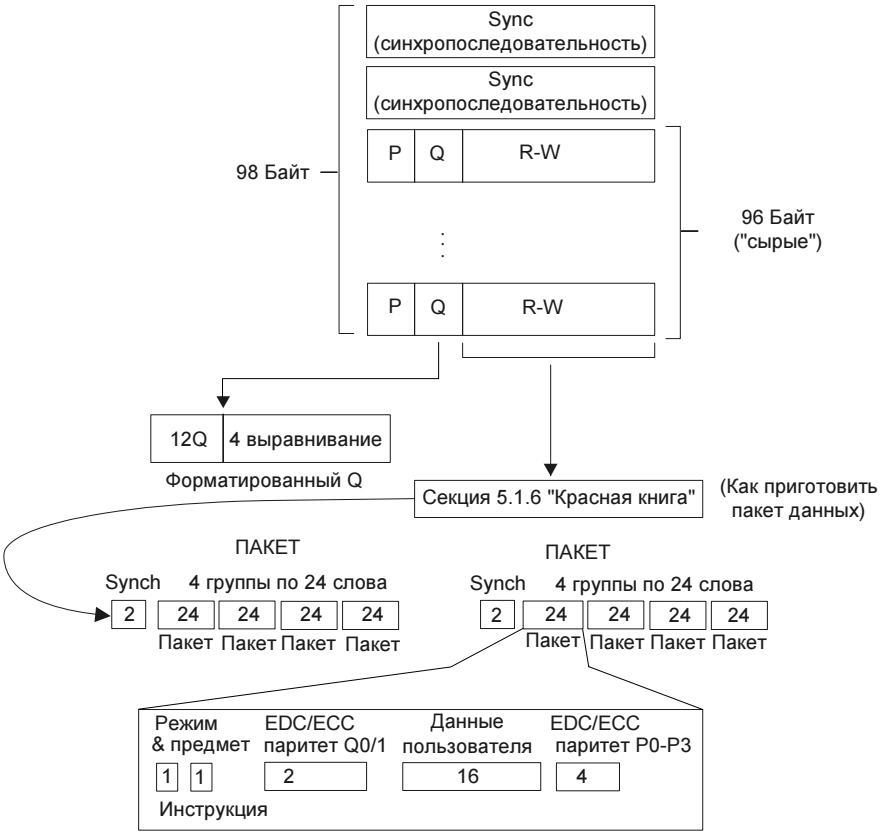


Рис. 1.6. Организация субканальных данных

Субканальные данные полностью изолированы от содержимого сектора и в некотором роде ведут себя точно так же, как и множественные потоки данных в файловой системе NTFS (читайте *"Основы Windows NT и NTFS"* Хелен Кастер). Все это наглядно иллюстрирует рис. 1.7.

Каждый из восьми битов, слагающих байт субкода, обозначается заглавной латинской буковой P, Q, R, S, T, U, V и W соответственно. Одноименные биты субканальных байтов всех фреймов объединяются в так называемые *каналы субкода*. Каналы состоят из *секций*, каждая из которых образуется путем объединения субканальных данных из 98 фреймов, что соответствует одному сектору (см. рис. 1.6). Однако границы секций и секторов могут и не совпадать, поэтому для гарантированного извлечения одной секции с диска мы должны прочесть два сектора. Первые два байта секции задействованы для синхронизации, а 96 отданы под действительные данные. Путем несложных расчетов можно вычислить, что на каждый канал приходится ровно по 16 байт "сырых", еще не обработанных данных.

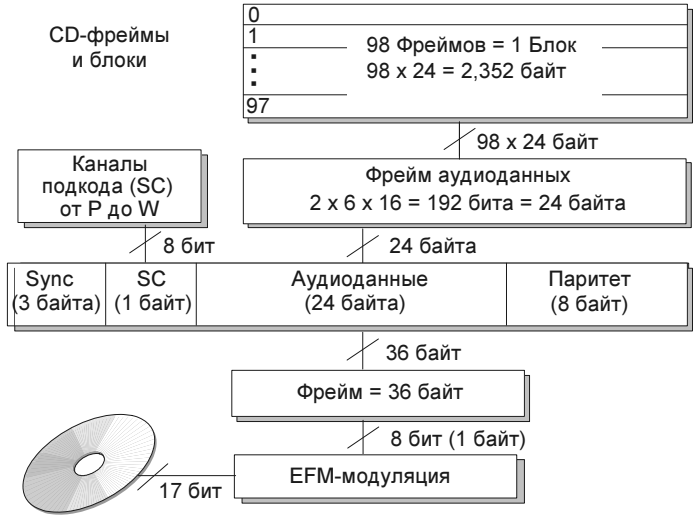


Рис. 1.7. Иерархия различных структур данных

Данные каналов P и Q поступают в виде, уже готовом к употреблению, причем значимыми из них являются только первые 12 байт, а остальные используются для выравнивания. Данные каналов P—W перед употреблением должны быть специальным образом "приготовлены" (cook). 96 составляющих их 6-битных *символов* разбиваются на 4-группы, состоящие их 24 слов. Каждое такая группа называется *пакетом* (pack) и включает в себя 16 символов пользовательских данных и 2 + 4 символа корректирующих кодов ECC/EDC *(Error Correcting Code/Error Detection and Correction)*.

Но что за информация хранится в каналах подкода? Согласно стандарту ECMA-130, "нормальные" компакт-диски задействуют лишь два канала: P и Q.

Канал P содержит в себе маркер окончания текущего трека и указатель на следующий трек, а *канал Q* используется для хранения сервоинформации, определяющей текущую позицию данного блока на диске, и является важнейшим каналом из всех.

Структурно канал Q состоит из следующих частей: *четырех управляющих битов*, соответствующих полю Control; *четырех адресных битов*, соответствующих полю q-Mode (ADR); *72 битов Q-данных*, соответствующих полю q-Data, и *16 битов контрольной суммы*, соответствующих полю CRC (рис. 1.8).

Таблица 1.1. *Формат данных Q-подканала*

Байт	Описание
0	Control/ADR
1	TNO (Track Number — номер трека)

Таблица 1.1 *(окончание)*

Байт	Описание	
2	INDEX (номер индекса)	
3	P-Min	Положение головки относительно начала трека (относительный адрес)
4	P-SEC	
5	Pframe*	
6	ZERO	
7	A-MIN	Положение головки относительно начала диска (абсолютный адрес)
8	A-SEC	
9	AFrame	
10	CRC	
11		
12	Оставлено для выравнивания	
13		
14		
15		

* В "Красной книге", соответствующей стандарту ECMA-130, данное поле именуется FRAC, а в SCSI Multimedia Commands/ATAPI DVD Devices — Frame, что создает определенные неудобства и терминологическую путаницу.

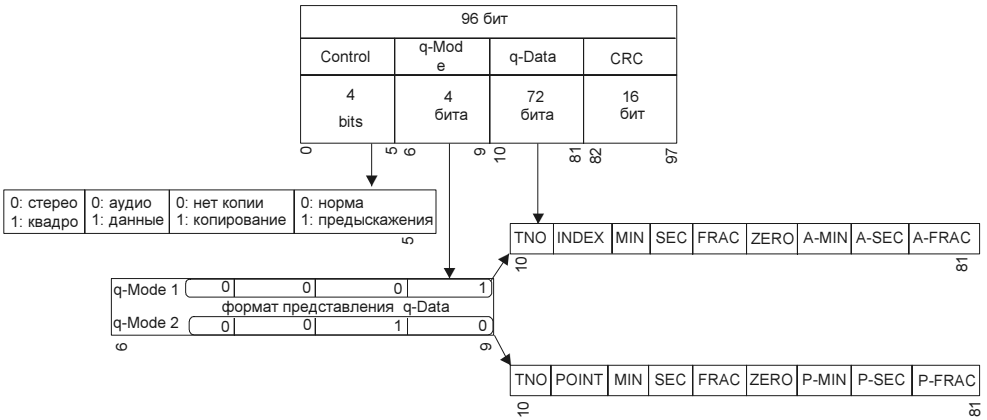


Рис. 1.8. Формат данных Q-подканала

Поле **Control** определяет содержимое трека (аудио или данные), количество аудиоканалов (стерео или квадро), а также указывает, разрешается ли копировать данные или нет. В частности, последовательность "0110" обозначает, что в пользовательской части сектора (user-data) записаны цифровые данные и их копирование не возбраняется. Напротив, последовательность "0100" запрещает копирование данных с диска. Другими словами, если третий слева, считая от нуля, т. е. 2 бит установлен, то копирование разрешено, и, соответственно, запрещено, если сброшен. Забавно, но большинство пишущих приводов всегда сбрасывает этот бит в ноль, даже если на диск записываются файлы, созданные самим пользователем. Впрочем, копировщики (в том числе и штатные) целиком и полностью игнорируют эти нелепые запреты, а потому конечный пользователь даже не догадываться о том, каких проблем он избежал!

Поле **q-Mode** определяет формат представления данных в поле **q-Data**, и для подавляющего большинства CD-ROM дисков оно равно единице.

Поле **q-Data** в режиме q-Mode == Mode 1 состоит из девяти однобайтовых полей, содержащих информацию о секторе (остальные режимы в силу их экзотичности не рассматриваются):

- **TNO** (Track **N**umber) — содержит в себе номер текущего трека, принимающий значения от 01 до 99; магическое число `0xAA` указывает на трек Lead-Out;
- **INDEX** — содержит в себе индекс текущей секции внутри текущего трека: 00 — указывает на паузу, значения от 01 до 99 идентифицируют секцию с полезными данными; однако в настоящее время эта возможность не используется и индекс секции всегда равен либо нулю (audio-pause), либо единице (actual data); индекс трека Lead-Out должен быть равен нулю;
- **MIN, SEC, FRAC** — время проигрывания сектора от начала текущего трека (минуты: секунды: фреймы соответственно), также называемое относительным временем проигрывания;
- **ZERO** — это поле должно всегда быть равно нулю;
- **A-MIN, A-SEC, A-FRAC** — время проигрывания диска от начала области данных (минуты: секунды: фреймы соответственно), также называемое абсолютным временем проигрывания.

Поле **CRC** содержит контрольную сумму содержимого *Q*-канала подкода и вычисляется по следующему полиному: $G(x) = x^{16} + x^{12} + x^5 + 1$.

Адресация секторов

Адресация сектора произошла от аудиодисков и записывается в формате Time — mm:ss:ff (минуты:секунды:доли, где доля в секунде равна от 0 до 74). Отсчет начинается с начала программной области, т. е. адреса секторов вводной области отрицательные.

Для перевода MSF[1]-адреса в LBA[2] можно воспользоваться следующей формулой: Logical Sector Address = (((Minute*60)+Seconds)*75) − 150.

"Сырые" и "сухие" сектора

IEC 908 — стандарт на аудиокомпакт-диски, вышедший в 1982 году в книге с красной обложкой (и потому вполне официально называемой *"Красной книгой" — Red Book*), описывал сектор как логический блок с длиной в 2352 байта, не имеющий никаких дополнительных полей и представляющий собой сплошной аудиопоток оцифрованной музыки. Что ж, логично! Сектора всех остальных накопителей (дискет, винчестеров) на логическом уровне устроены совершенно аналогично и различаются разве что длиной (в частности длина сектора гибких/жестких дисков равна 512 байтам).

К сожалению, попытка непосредственного использования аудиодиска для хранения данных потерпела неудачу. Слишком высокая плотность записи вкупе с техническим несовершенством механизма чтения привели к тому, что при воспроизведении диска постоянно возникали ошибки, количество которых на 10-секундном участке трека могло доходить до двухсот! Для аудио это вполне нормально (что русскому хорошо, то немцу — смерть), поскольку сбойные биты легко выправляются интерполяцией, и хотя достоверность воспроизведения аудиопотока при этом уже не гарантируется, человеческое ухо (даже хорошо тренированное!) все равно не замечает разницы, а потому увеличение плотности записи в угоду емкости диска вполне оправданно.

Естественно, для исправления ошибок, возникающих при чтении файлов данных, методика интерполяции абсолютно непригодна, и с вероятностью, близкой к единице, считанный файл окажется безнадежно изуродованным. Для решения этой проблемы пришлось увеличить избыточность записываемой на диск информации и ввести дополнительные корректирующие коды. По соображениям совместимости с уже имеющимся оборудованием (и производственными мощностями в том числе!) существующий формат хранения информации был полностью сохранен, но к нему добавился еще один уровень абстракции.

Стандарт *"Желтой книги"* (*Yellow Book*), вышедший в 1983 году, описывает сектор как сложную структуру, состоящую из 12-байтовой синхропоследовательности, 4-байтового заголовка, 2048-байтовой области данных, 4-байтового поля кода коррекции EDC, 8-байтовой вспомогательной области (Auxiliary) и 276-байтового поля кода коррекции ECC (рис. 1.9).

Естественно, аппаратная начинка привода CD-ROM скрывает все эти подробности и выдает содержимое служебных полей только по специальной

[1] MSF — Minutes Second Frame, минуты : секунды : фреймы.
[2] LBA — Logical Block Address.

команде (которую, кстати говоря, поддерживают не все модели). С программистской точки зрения, 2048 байта пользовательской области данных — это и есть та минимальная порция информации, с которой штатный привод может работать. Замечательно, что в результате урезания "настоящего" сектора, длина логического сектора оказалась кратной размеру секторов остальных устройств! Так какие проблемы и зачем, срывая уровни абстракции, лезть куда-то вглубь? А вот зачем. Манипулируя служебными полями, вы можете как создавать диски, не копируемые штатными средствами, так и взламывать защитные механизмы, препятствующие несанкционированному копированию.

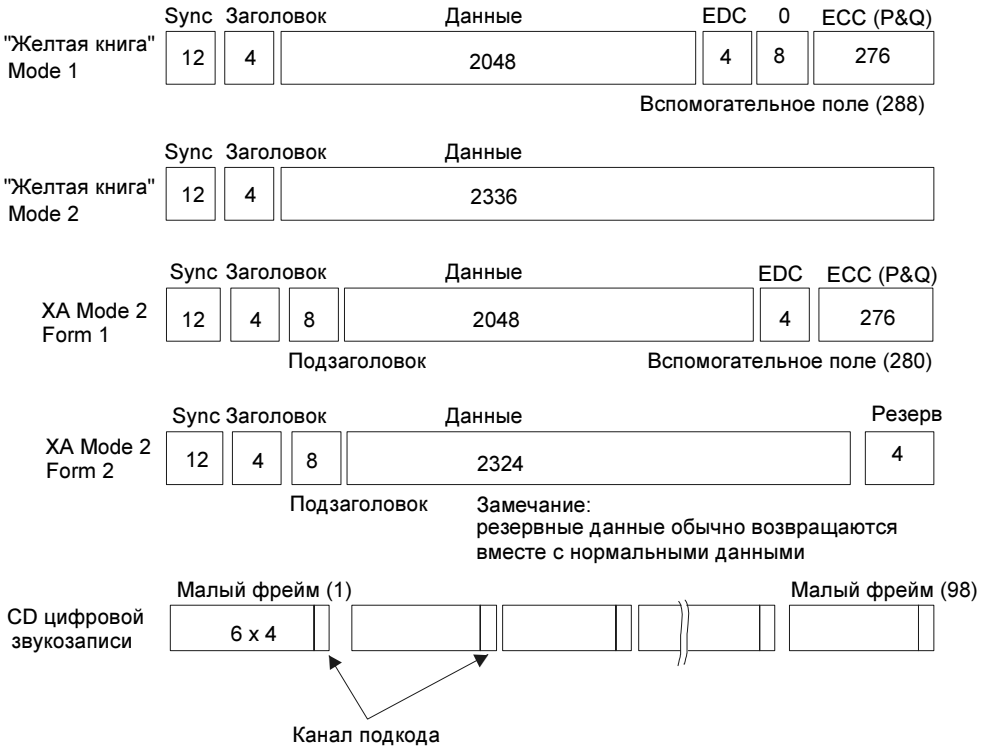


Рис. 1.9. Сектора различных типов

Если вы еще не особенно утомились сухой теорией, то совершим еще один рывок и рассмотрим формат сектора для режима MODE 1 (рис. 1.10) (на случай вашего воодушевления хочу сказать, что теория скоро закончится и начнется увлекательный процесс исследования диска под "микроскопом").

- Поле *синхронизации* (Sync) состоит из следующей последовательности: 00h FFh FFh FFh FFh FFh FFh FFh FFh FFh FFh 00h и служит индикатором начала сектора.