

Надежность гелиевых дисков: классика и современность

Илья Манусов



Появление [гелий-наполненных магнитных дисков](#) и, как следствие, существенное увеличение плотности записи, порождает ряд новых факторов, определяющих надежность хранения данных. Решения, предлагаемые производителями, можно разделить на две группы: к первой отнесем совершенствование классических технологий, существующих уже десятилетия, например, *циклический контрольный код (CRC)* и *код коррекции ошибок (ECC)*. Ко второй группе относятся решения, логика которых прямо связана с наличием гелия в гермокамере, например, датчик, анализирующий состав атмосферы внутри устройства и доступный как [SMART-атрибут с идентификатором ID=22h](#).

Фундаментальные принципы надежности

Процесс чтения данных с носителя, может привести к одному из трех результатов:

1. *Информация прочитана успешно, без искажений.*
2. *Информация прочитана с ошибками, ошибки обнаружены. Факт сбоя обнаружен при проверке циклической контрольной суммы данных и стал известен хост-системе посредством опроса статуса накопителя.*
3. *Информация прочитана с ошибками, ошибки не обнаружены, хост система интерпретирует искаженные данные как корректные.*

Понимая физические принципы работы магнитных дисков, на ситуацию (2) разработчики всегда смотрели «философски», некоторая вероятность сбоя существует неизбежно. Гораздо важнее предотвратить ситуацию (3), так как, например, передача управления на искаженный выполняемый файл приведет к непредсказуемым последствиям, не говоря уже о незаметной подмене информации в научных расчетах или финансовой аналитике.

Упрощенно, защита информации реализуется следующим методом:

- *при записи сектора на диск, контроллер вычисляет CRC-код как функцию от содержимого поля данных сектора и дописывает вычисленное значение после сектора;*
- *при чтении сектора с диска, контроллер также вычисляет CRC-код, но уже для читаемых данных и сравнивает его с содержимым поля CRC, сформированного при записи. В случае несовпадения, становится известно об ошибке.*

Почему защита не всесильна

Для определенности, рассмотрим сектор, размером 512 байт, снабженный контрольным кодом размером 4 байта.

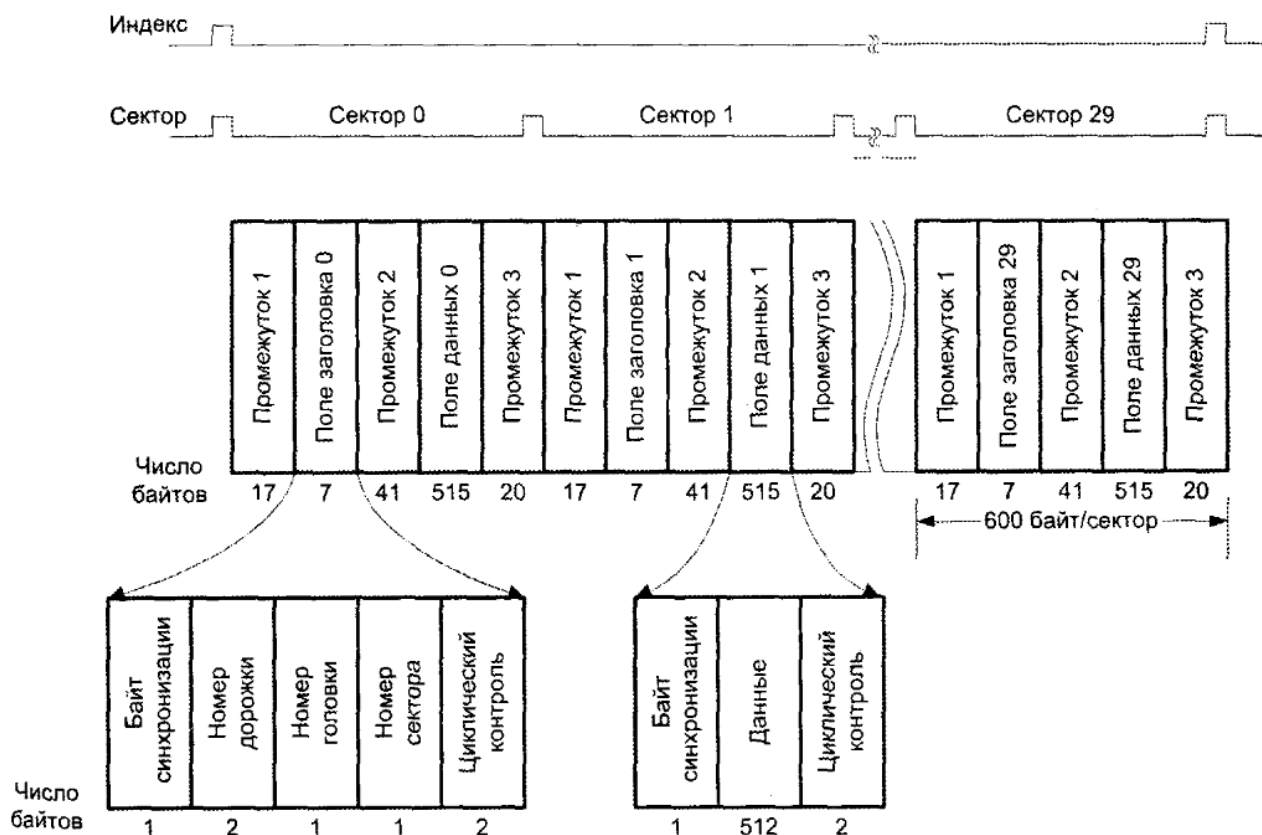


Рис 1. Формат дорожки, используемый в накопителях Seagate ST506

«Наивно-ностальгический» вариант 512+4 (рис.1) мы избрали исключительно для того, чтобы упростить рассмотрение математических принципов, лежащих в основе контрольных кодов. В жизни все сложнее: *физическая* и *логическая* геометрия накопителей не совпадает еще со времен IDE устройств, поэтому вряд ли сегодня можно обнаружить секторы такого размера на поверхности диска. Кроме того, индустрия с переменным успехом пытается перейти от 512-байтных логических секторов к 4096-байтным, один из аргументов такого шага состоит в приведении в соответствие размера сектора и размера страницы виртуальной памяти.

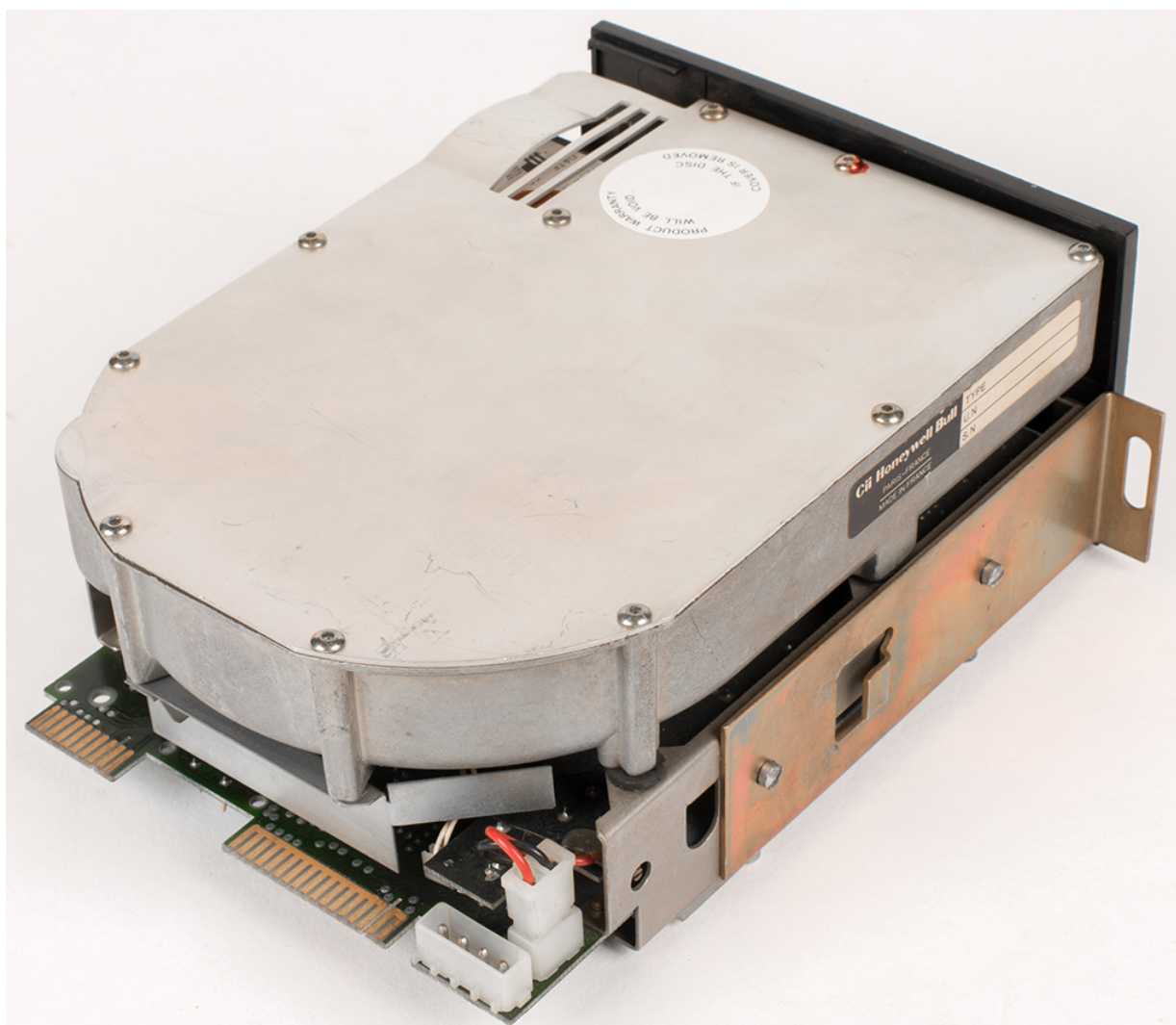


Рис 2. Накопитель на жестких магнитных дисках Seagate ST506

Итак, у нас 512 байт данных и 4 байта $CRC=F(DATA)$, сформированные, как функция от 512 байт данных. Всего $512*8 + 4*8 = 4128$ бит. Такой битовый вектор может иметь гигантское значение состояний, равное (*2 в степени 4128*). Обозначим это полное множество значений составного поля DATA+CRC как X .

По отдельности, поле данных может иметь (*2 в степени 4096*) состояний, поле CRC может иметь (*2 в степени 32*) состояний. Каждому правильно вычисленному значению $CRC=F(DATA)$ соответствует не один, а множество вариантов значений поля данных. Именно этим обусловлена вероятность возникновения *узаконенных* ошибок, при которых прочитанные данные имеют расхождения с записанными, тем не менее CRC корректно.

Подмножество множества X , для которого соотношение $CRC=F(DATA)$ верно, обозначим как Y . В силу того, что множество Y содержит более одного элемента, существует вероятность необнаруженных ошибок. Единственно правильный вариант, или оригинальные записанные данные, обозначим как Z . Тогда справедливо следующее:

Если в результате искажения, значение Z останется элементом подмножества Y, ошибка не будет обнаружена, так как соотношение $CRC=F(DATA)$ останется верным. Иначе, ошибка будет обнаружена.

Качество контрольного кода определяется *кодowym расстоянием*. Этот параметр определяет количество битов, которые должны быть искажены для получения не обнаруживаемой ошибки. При заданном кодовом расстоянии N , любые два элемента множества Y , должны различаться минимум в N битах.

Резюме

Циклические контрольные коды применяются уже несколько десятилетий с момента появления первых устройств хранения данных. Такие новшества, как наличие гелия в гермокамере, не изменяют фундаментальных математических законов данного вида защиты. С другой стороны, повышение плотности записи, расширение списка факторов, влияющих на надежность чтения и записи информации, предъявляют новые требования к технологиям обнаружения и исправления ошибок.

В свою очередь, увеличение доли объема носителя, отводимой для контрольных кодов может несколько нивелировать эффект повышения плотности записи. Перед разработчиками, как обычно, стоит задача нахождения оптимального компромисса.