3. Вертикальный и горизонтальный контроль по паритету. Исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы.

4. Коды Хэмминга. Самостоятельно находят и исправляют ошибки, даже изолированные, то есть искаженные отдельные биты которые могут быть разделены большим количеством правильных битов.

Построение кодов Хэмминга основано на принципе проверки на четность числа единичных символов: к последовательности добавляется такой элемент, чтобы число единичных символов в получившейся последовательности было четным, ($S = 0$ – ошибок нет, $S = 1$ – однократная ошибка). Матрица преобразования соответствующей размерности умножается на матрицу-столбец кодового слова и каждый элемент полученной матрицы-столбца берется по модулю 2. На аппаратном уровне, в Optix OSN 8800, коды Хэмминга реализуются в модуле OTN tributary unit, на плате TN52TOG.

ИСПОЛЬЗОВАНИЕ ЖУРНАЛА ИЗМЕНЕНИЙ ФАЙЛОВ NTFS В КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

О.Р. Мысливец

При проведении компьютерно-технической экспертизы, а именно при анализе файловой системы NTFS, часто встает необходимость в поиске удаленных файлов и их анализе. Несмотря на то, что методы поиска удаленных файлов и их восстановления для файловой системы NTFS [1] не представляют особой сложности, не всегда возможно полностью восстановить файл для последующего анализа. В подобных случаях, если не удается восстановить файл полностью либо частично, существует возможность получить информацию о том, хранился ли файл в файловой системе в определенный промежуток времени и определить действия, проводимые над файлом. Информацию такого рода можно получить из журнала изменений файлов NTFS. Наряду с именами файлов и информацией об их MFT-записях, данный метафайл хранит в себе информацию о действиях, произведенных над файлами, а также временные метки произведенных действий [2]. С помощью данной информации можно однозначно установить факт хранения и использования некоторого файла, вплоть до получения полной последовательности произведенных над файлом действий за определенный промежуток времени. Недостатками данного подхода можно считать возможное отсутствие метафайла, вследствие его преднамеренного удаления или отключение опции журналирования для конкретного тома, а также ввиду ограничений на размер журнала изменений файлов, некоторые записи в журнале могут быть перезаписаны более новыми, что может повлиять на конечный результат. Несмотря на все недостатки данного подхода, в ходе исследований выяснилось, что в процессе анализа журнала изменений файлов NTFS существует вероятность получения информации о файлах, удаленных более 3 месяцев назад, но и не более 6 месяцев с момента удаления при условии активного использования накопителя информации.

Литература

1. Кэрриэ, Б. Криминалистический анализ файловых систем/ Кэрриэ Б. – СПб.: Питер, 2007. – 470 с.

2. USN_RECORD_V2 structure [Электронный ресурс] / Microsoft TechNet – Режим доступа: https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa365722(v=vs.85).aspx – Дата доступа: 17.05.2017.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ХРАНЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ БАЗЫ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Е.А. Нестерович, С.А. Зайкова

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в настоящее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных (СУБД), в особенности реляционные, стали доминирующим инструментом в этой области. Обеспечение информационной безопасности СУБД приобретает решающее