

Ю.В. Гольчевский, В.Н. Тропников

*Сыктывкарский государственный университет
им. Питирима Сорокина, г. Сыктывкар*

ПРОБЛЕМА ГАРАНТИРОВАННОГО УНИЧТОЖЕНИЯ ИНФОРМАЦИИ В БАЗАХ ДАнных: ПОДХОД НА ОСНОВЕ РАБОТЫ С ФАЙЛАМИ ДАнных

Проблема гарантированного уничтожения информации (ГУИ) обычно решается с помощью средств защиты информации (СЗИ). При этом, преимущественно, речь идет об удалении остаточной информации от целых файлов, а не частей файлов, как, например, кортежей в базах данных (БД). Особенность в том, что при удалении записей в БД происходит не удаление файла, а изменение, что не позволяет СЗИ затереть удаляемую информацию в соответствии с требованиями руководящих документов. Существует ряд исследований в этой области, например [1; 2], но проблема остается до сих пор открытой.

Чтобы обеспечить ГУИ в БД необходимо выполнить два условия. Первое – не должна появляться остаточная информация на страницах БД, второе – не должна появляться остаточная информация в файловой системе. Можно предложить два способа. Первый – расширение функционала систем управления базами данных (СУБД). Для этого необходимо изменить работу команд СУБД, в результате выполнения которых может появляться остаточная информация. Второй – создание программы, которая будет работать непосредственно с файлами таблиц, и затирать в них остаточную информацию согласно предъявляемым требованиям.

Возможные методы расширения функционала СУБД подробно описаны в работе [1]. Требуется реализовать интерфейс определения пользователем настроек безопасности БД, реализовать алгоритм перезаписи данных для команд, приводящих к возможности появления остаточной информации и выбор требуемого алгоритма пользователем. Кроме того необходимо определить процесс выбора

пользователем создания обычной или защищенной таблицы. Главное преимущество реализации ГУИ данным способом – доступность информации, содержащейся в БД. Основной недостаток – значительное падение производительности СУБД при выполнении многократной перезаписи.

При непосредственной работе с файлами данных уничтожение остаточной информации производится не средствами СУБД, а сторонней программой. В ходе исследования была разработана программа, осуществляющая очистку файлов данных таблиц MySQL. Считываются номера секторов, которые занимает файл таблицы, затем выполняется чтение файла. Данные первого сектора, принадлежащего файлу, заносятся в кэш программы и производится поиск остаточной информации. Если она обнаружена – производится затирание в соответствии с выбранным алгоритмом, иначе в кэш загружается следующий сектор и алгоритм возвращается к третьему шагу. Это повторяется, пока не будут проверены все секторы файла таблицы.

Основную сложность составляет алгоритм поиска остаточной информации. Если запись таблицы располагается более, чем в одном секторе, возникает необходимость считывать ее заголовки, чтобы это обнаружить. Иначе очистка будет произведена неправильно и БД будет повреждена. Вторая проблема, требующая проработки – отслеживание дискового пространства, освобождаемого при оптимизации таблиц БД. Еще одна особенность состоит в том, что при прямой работе с файлами данных могут появляться расхождения с журналами транзакций. Восстановление состояния БД в соответствии с журналами будет невозможно. То есть для последующей корректной работы пользователя с БД недостаточно только изменять сами данные, но и возникает необходимость соответствующим образом модифицировать и файлы журналов.

В отличие от предыдущего, данный метод не приводит к падению производительности СУБД. Положительной стороной является и ситуативность его использования. Основной недостаток – временная потеря доступа к данным. Стоит заметить, что при работе с большой БД очистка может занять достаточно продолжительное время.

Анализ результатов работы разработанной программы позволяет сделать вывод, что данный метод может эффективно применяться для уничтожения остаточной информации.

Литература

1. *Grebhahn A., Schaler M., Koppen V.* Secure Deletion: Towards Tailor-Made Privacy in Database Systems. URL: http://www.iti.cs.unimagdeburg.de/iti_db/publikationen/ps/auto/GSK13.pdf.
2. *Diesburg S.M., Wang A.A.* A Survey Of Confidential Data Storage And Deletion Methods // ACM Computing Surveys. 2010. Vol. 43, № 1. P. 2:1–2:27.