# АВТОМАТИЗИРОВАННАЯ ОБУЧАЕМАЯ СИСТЕМА ЗАЩИТЫ ОТ SQL-ИНЪЕКЦИЙ

С.С. Куликов, Н.В. Манько, Ю.А. Петранков

Предлагаемый метод основан на статистическом анализе обращений к базе данных с последующим формированием "профиля атаки" и его использованием для защиты БД от SQL-инъекций.

На первом этапе система проходит обучение "с учителем". В роли "учителя" выступает выражение, включающее в себя: имя файла, посредством которого был выполнен запрос, тип запроса, структуру запроса (операторы, названия таблиц и полей, задействованных при формировании запроса). На данном этапе в набор собираемых статистических данных включаются все запросы, выполняемые пользователем.

Встраивание системы защиты в базу данных происходит посредствам триггеров и хранимых процедур.

На втором этапе анализируется тип и структура запросов к базе данных на основе стандарта SQL; анализируются все файлы, из которых были произведены запросы.

На третьем этапе система активизируется, анализируя каждый входящий запрос. Если файл, в котором выполнялись запросы типа SELECT, присылает запрос любого другого типа (структуры), запрос отклоняется и система уведомляет администратора об ошибке. В случае подтверждения администратором блокирования запроса, он сохраняется в списке запрещённых, в противном случае — включается в список разрешённых.

Несмотря на затраты производительности, данный метод позволяет значительно сократить исправления, вносимые в программный код защищаемого продукта.