УДК 004.056

Разработка базы данных для средства моделирования угроз газодобывающих предприятий

А.С. Римша (АО Ачимгаз, г. Новый Уренгой)
К.С. Римша (Тюменский Государственный университет, г. Тюмень)
А.А. Захаров (Тюменский Государственный университет, г. Тюмень)

В статье рассматривается структура базы данных для разрабатываемого средства моделирования угроз и оценки рисков информационной безопасности автоматизированной системы управления технологическими процессами. Предлагаемая структура базы данных учитывает специфические особенности типовых АСУ ТП, относящихся к категории опасных производственных объектов. Одна из причин аварийных ситуаций может быть связана с недостаточной защищенностью АСУ ТП. В связи с этим актуальной задачей является обеспечение корректности проводимой оценки рисков существующих угроз. Проведено сравнение наиболее популярных свободно распространяемых СУБД, на основе которого выбирается наиболее подходящая система. Рассмотрена структура базы данных, используемая для разрабатываемого средства моделирования угроз. Описан процесс пополнения базы данных существующими уязвимостями из общедоступных источников. Приведены основные формулы для расчета оценки рисков. Разрабатываемое решение позволяет автоматизировать процесс оценки рисков по задаваемой топологии АСУ ТП.

Модернизация подходов к обеспечению ИБ АСУ ТП предполагает изменение стратегии и тактики проводимых работ для построения эффективной системы защиты в соответствии с моделью угроз и возможными сценариями атак - от кибернападений до аварий.

Большинство решений на рынке для обеспечения ИБ автоматизированных систем представляют собой как программные, так и аппаратные инструменты, которые для реализации своего функционала требуют интеграции в промышленную сеть. Учитывая, что АСУ ТП, как правило, представляет собой непрерывный процесс, внедрение подобных средств обеспечения ИБ в системах, в которых изначально не было предусмотрено и протестировано их использование, может неблагоприятно повлиять частично или полностью на весь технологический процесс. Такие проблемы могут быть вызваны, как несовместимостью оборудования или ПО, так и встроенным функционалом блокирования этих средств. Исходя из того, что АСУ ТП чаще всего является опасным промышленным объектом, подобное воздействие может быть причиной отказа оборудования или даже аварии, поэтому при выборе решений для защиты системы необходимо руководствоваться в первую очередь минимальным вмешательством в производственные процессы.

Одним из наиболее подходящих инструментов, не требующим вмешательства в производственные процессы, является средство моделирования угроз. Отсутствие свободно распространяемых средств моделирования угроз, ориентированных именно на промышленные сети, свидетельствует о необходимости разработки подобного решения. Для работы средств моделирования угроз необходимо хранить и поддерживать актуальные сведения о существующих угрозах. Таким образом, в данной статье будет изложена предлагаемая структура базы данных для разрабатываемого средства моделирования угроз.

Перед разработкой такого сложного продукта, как средство моделирования угроз, необходимо определиться с хранением и актуальным содержанием БД, с которым будет работать приложение.

В результате работы была разработана структура БД, которая позволяет эффективно хранить и пополнять данные с указанных ресурсов. Также данная структура позволяет в случае появления дополнительных параметров или ресурсов дополнить БД новыми таблицами, не нарушая при этом логику приложения.

Данная структура была использована в разработанном авторами приложении, что позволило провести анализ рисков АСУ ТП газодобывающего предприятия.