ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КОМБИНИРОВАННОГО МЕТОДА ОЦЕНКИ ЗАЩИЩЕННОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Е.В. Шакун

Программа реализует комбинированный (с позиций используемых показателей и объекта оценки) метод, сущность которого состоит в следующем.

Исходными данными для оценки являются:

• пригодный для тестирования объект с документацией к нему, разработанный на основе требований задания по безопасности, которое соответствует одному из уровней гарантии оценки (УГО) от первого (УГО1) до четвертого (УГО4);

• база знаний, содержащая множество единиц работы по проверке соответствия объекта требованиям безопасности с комментариями к единицам работы. Каждая из единиц работы относится к определенным подоперациям (компонентам гарантии), которые, в свою очередь, объединены в операции (классы гарантии).

Комбинированный метод оценки защищенности объектов информационных технологий (ОИТ) на соответствие требованиям задания по безопасности, заключается в следующем:

• установлении для каждой единицы работы, подоперации и операции количественного значения оценки важности (веса);

• анализе единиц работы с целью проверки степени реализации в объекте требований безопасности и установлении количественного значения оценки качества каждой единицы работы;

• последовательном вычислении качества подоперации в виде взвешенных аддитивных сверток оценок качества соответствующих единиц работы;

• последовательном вычислении качества операций в виде взвешенных аддитивных сверток оценок качества соответствующих подопераций;

• оценке степени защищенности ОИТ в виде взвешенных аддитивных сверток множества оценок качества операций;

• формировании экспертного лингвистического заключения о степени защищенности ОИТ с использованием интервального решающего правила.

При проведении оценки защищенности ОИТ используются базы знаний, обеспечивающие поддержку принятия решений, в том числе:

• база знаний, создаваемая в результате накопления информации об ОИТ, прошедших процедуру оценки защищенности, и содержащая статистическую информацию о них;

• база знаний множества единиц работы, подопераций и операций для одного из четырех уровней гарантии оценки, а также комментарии и рекомендации по единице работы и использующаяся при оценке соответствия требованиям безопасности;

• база знаний накопленного опыта (протоколов испытаний), полученного путем использования результатов предыдущих оценок защищенности ОИТ и использующаяся для сравнения принимаемого решения по качеству рассматриваемой единицы работы с решениями, принятыми ранее по объектам, имеющим наиболее высокий уровень защищенности.

Программная реализация предлагает вариант клиент серверного построения приложения, базирующегося на локальной сети организации. На сервере располагаются базы знаний и данных, на клиентских компьютерах — непосредственно система.

В системе предусмотрена процедура авторизации, с использованием фамилии эксперта (логин) и пароля, которая может осуществляться в роли администратора системы или эксперта.

Роль администратора имеет полный спектр полномочий действий над системой. Она позволяет регистрировать новые документы в базе знаний и удалять их, редактировать информацию о документах, значения шкал весов и оценок, добавлять материал в базы знаний. Также только администратор системы может задать веса для единиц работы, подопераций и операций. Роль эксперта позволяет использовать базы знаний, работать с существующими документами, проводя их оценку.

При регистрации нового объекта необходимо ввести его краткое и полное название, данные и реквизиты заказчика, задать шкалы весов и оценок. Изначально шкалы сформированы по умолчанию, пользователь может изменить их по своему желанию.

Непосредственное окно для работы по испытанию объекта делится на 4 части. В первой части проводится оценка единиц работы, во второй — подопераций, в третьей — операций, четвертая часть используется для проведения функционального тестирования объекта.

Если все этапы испытания объекта пройдены, система может посчитать итоговую оценку соответствия заданию по безопасности. Также по результатам испытаний пользователь может составить отчет, используя сохраненные в системе данные.

Поддержка принятия решений в системе реализована в виде отдельного окна, ее использование описано в разделе описания метода. В режиме эксперта доступны только данные оценок, проводимых непосредственно этим экспертом, в режиме администратора доступны также данные других экспертов, зарегистрированных в системе.

Использование баз знаний для поддержки принятия решений в разработанном комбинированном методе оценки защищенности ОИТ позволяет не только повысить адекватность формируемых экспертных заключений, но и, в случае вынесения отрицательного заключения, выявить слабые стороны оцениваемого объекта и указать пути дальнейшей доработки и совершенствования.