ПОДХОД К ВЫБОРУ ТРЕБОВАНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ КЛАСТЕРНОГО АНАЛИЗА

В.А. КОРЛУЖЕНКО, Е.П. МАКСИМОВИЧ, В.К. ФИСЕНКО

При разработке профилей защиты или заданий по безопасности ключевое значение имеет определение набора требований безопасности (ТБ). Предлагается подход к выбору типового набора ТБ, основанный на экспертном анализе и классификации объектов информационных технологий (ОИТ) относительно предварительно сформированного множества кластеров. Определение множества кластеров сводится к задаче классификации без учителя и с внешней целью.

Реализация подхода разбивается на следующие основные этапы.

1. Построение множества общесистемных признаков для описания ОИТ. Признаки определяются на экспертном уровне и представляют собой лингвистические переменные (ЛП) типа "категория обрабатываемой информации", "условия функционирования ОИТ" и т.д.

2. Формирование множества допустимых ОИТ в терминах введенных признаков. На основании экспертного анализа строится иерархическое дерево. Корень дерева отождествляется со всеми ОИТ. Первое ветвление ведется по 1-му признаку — количество узлов 1-го уровня равно количеству термов (значений) ЛП 1-го признака. От узлов 1-го уровня проводится ветвление по 2-му признаку, учитывая все допустимые возможности. От узлов 2-го уровня — по третьему признаку и т.д. Множество концевых узлов дерева — все допустимые (с учетом предков) ОИТ.

3. Разбиение множества допустимых ОИТ на кластеры. На основе экспертного анализа производится последовательное продвижение сверху вниз по дереву. Корню дерева ставятся в соответствие все классы функциональных ТБ "Общих критериев". Если на некотором уровне выявляются узлы, которым соответствуют заведомо разные ТБ, то соответствующие им ОИТ относятся к разным кластерам. С каждым узлом связывается множество допустимых ТБ. В результате полного просмотра дерева формируется разбиение на кластеры. Каждому кластеру ставится в соответствие множество допустимых ТБ – все ТБ, которые не были отброшены в процессе рассмотрения предков соответствующего узла.

4. Формирование описания кластеров. На основе экспертного анализа для каждого кластера формируются (в терминах термов ЛП признаков) системы продукционных правил. В соответствии с критерием разбиения, любые два кластера отличаются значением хотя бы одного из признаков, вследствие чего для них можно определить разные правила.

5. Построение решающего правила. Правило состоит в проверке для ОИТ продукционных правил каждого кластера и отнесение объекта к тому кластеру, чьи правила для него выполняются.