ОБ ОДНОМ ПОДХОДЕ К ПРИНЯТИЮ РЕШЕНИЙ ПРИ ИСПЫТАНИИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В.В. Анищенко, Е.П. Максимович, В.К. Фисенко

Объединенный институт проблем информатики НАН Беларуси,
лаборатория проблем защиты информации
220012, г. Минск, ул. Сурганова, 6
+ (375 17) 284-21-22; e-mail: fisenko@.bas-net.by

Предлагается общий подход к построению системы поддержки принятия решений, предназначенной для автоматизации процесса оценки безопасности объектов информационных технологий и основанной на использовании методов нечеткой формализации, которые позволяют учесть субъективность и неточность экспертных оценок, используемых в качестве исходных данных для вынесения общего заключения о защищенности объекта.

Ключевые слова – единица работы, задание по безопасности, объект информационных технологий, уровень гарантии оценки.

ВВЕДЕНИЕ

Оценка безопасности объектов информационных технологий (ОИТ) – актуальное направление защиты информации. На практике оценка информационной безопасности конкретного ОИТ осуществляется коллективом экспертов и представляет собой сложный наукоемкий процесс, регламентированный соответствующими международными и национальными стандартами (ISO/IEC 18045 [1], «Общие критерии» [2]).

Оценка осуществляется на соответствие различным уровням гарантии оценки (УГО), в зависимости от природы рассматриваемого ОИТ и критичности используемой информации. Процесс оценки состоит в выполнении экспертами весьма большой совокупности различных единиц работы, содержание которых определяется требованиями компонентов гарантии соответствующего УГО и спецификой испытываемого ОИТ.

Для каждого конкретного ОИТ в качестве руководства по выполнению единиц работы экспертами должна быть разработана специальная рабочая методика, согласующаяся со стандартами и учитывающая специфику объекта. Результатом оценки должно быть экспертное заключение о качестве защищенности ОИТ.

Реализация указанного подхода требует от эксперта решения целого ряда нетривиальных задач, базирующихся на анализе существующих для ОИТ рисков безопасности и требующих учета большого количества плохо формализуемых, различных по своей значимости показателей. Слишком большое влияние субъективного фактора, а также отсутствие эффективных методов обработки больших объемов экспертных данных существенно снижают адекватность оценки, что обусловливает актуальность формализации и автоматизации процесса оценки. В докладе предлагается подход к построению системы поддержки принятия решения (СППР), направленный на автоматизацию процесса оценки безопасности ОИТ и основанный (в виду плохой формализуемости предметной области) на нечеткой формализации и использовании накопленного опыта.

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПОДХОДА

В рамках предлагаемого подхода рассмотрены следующие основные задачи оценки безопасности ОИТ:

- разработка рабочей методики оценки на основе разработки типовых методик оценки на соответствие ОИТ УГО1-УГО4 и использовании накопленного опыта оценки разных типов ОИТ;
- разработка гибкой пятибалльной системы лингвистических оценок, отражающей разную степень возможной защищенности ОИТ (вместо существующей в настоящее время слишком грубой двухбалльной системы «пригоден -не пригоден»);
- разработка методов обработки больших массивов экспертных оценок с целью вынесения интегрального заключения о безопасности ОИТ.

Процесс оценки включает следующие основные этапы:

- анализ предоставленных для оценки исходных данных и принятие ОИТ на испытание;
- оценка задания по безопасности (если оно до этого не было оценено);
- разработка рабочей методики на базе уточнения и конкретизации стандартизированной типовой методики оценки ОИТ соответствующего типа;
- автоматизированное испытание ОИТ отдельными независимыми экспертами, включая автоматическую обработку формируемой экспертом совокупности оценок по единицам работ и выработку интегрального заключения;
- автоматизированная выработка коллективного экспертного решения, осуществляемая под управлением руководителя испытаний;
- автоматизированное оформление результатов оценки.

Для реализации трех первых этапов в рамках подхода разработаны соответствующие типовые методики. Для реализации остальных этапов разработана пилотная версия специализированной СППР.

2 СТРУКТУРА СППР

Общая структура разработанной СППР приведена на рис.1.

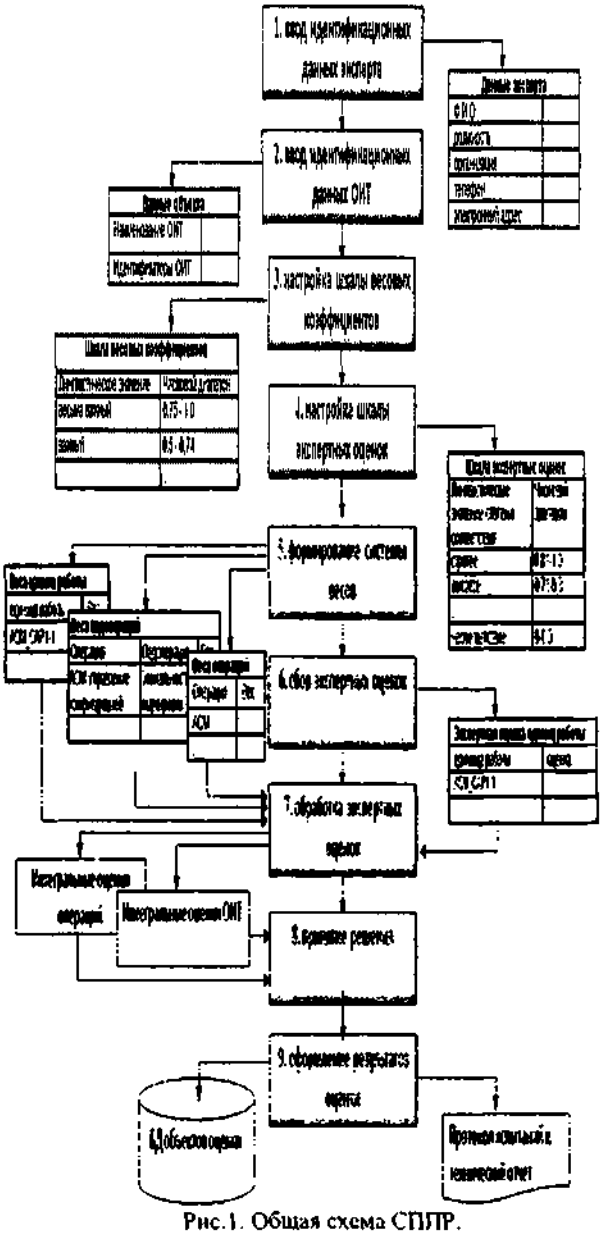

Рис.1. Общая схема СППР.

В рамках СППР поддерживаются две роли пользователей: – независимый эксперт и руководитель испытаний. Пользователь-эксперт использует СППР для автоматизированного проведения независимой оценки ОИТ и выработки личного заключения о безопасности ОИТ. Пользователь-руководитель испытаний использует СППР для общего руководства процессом оценки и выработки общего согласованного заключения о безопасности ОИТ коллективом экспертов.

СППР обеспечивает решение следующих основных задач:

– реализация и настройка комбинированной шкалы оценки (интервалов количественных оценок, соответствующих лингвистическим оценкам);

– обеспечение справочных руководств по выполнению регламентированных единиц работы на основе действующих стандартов и накопленного опыта оценки разных типов ОИТ;

- ранжирование единиц работы, операций и подопераций по их значимости при оценке безопасности ОИТ;

– автоматизация процесса экспертной оценки регламентированной совокупности единиц работы и определения уточняющих числовых значений по каждой единице работы;

– определение количественной интегральной оценки безопасности ОИТ на основе формирования иерархической трехуровневой системы взвешенных аддитивных сверток для подопераций, операций и ОИТ в целом;

– определение интегральной лингвистической оценки безопасности ОИТ на основе методов интервальной оценки;

– поддержка управления процессом со стороны руководителя испытаний, включая автоматизацию процесса выработки общего коллективного заключения группой независимых экспертов;

– автоматизация формирования протоколов оценки.

ЗАКЛЮЧЕНИЕ

Практическое значение СППР, реализующей предложенный подход состоит в том, что она позволяет обеспечить соответствие процесса оценки действующим стандартам, существенно снижает трудоемкость данного процесса, повышает точность и обоснованность результатов оценки, позволяет накапливать и эффективно использовать опыт испытания разных типов ОИТ.

ЛИТЕРАТУРА

[1] ISO/IEC 18045:2005(E). Information technology – Security techniques Methodology for IT security evaluation – 286 p.

[2] СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999). Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Часть 3: Гарантийные требования безопасности 114 с.