ИНФОРМАТИКА

2009 **июль-сентябрь** **№ 3**

ЗАЩИТА ИНФОРМАЦИИ

УДК 681.03

В.В. Анищенко, В.К. Фисенко, Е.П. Максимович, М.С. Шибут

АВТОМАТИЗАЦИЯ ПРОЦЕССА ОЦЕНКИ БЕЗОПАСНОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Предлагается подход к автоматизации процесса оценки безопасности объектов информационных технологий на соответствие требованиям Общих критериев, основанный на нечеткой формализации и использовании накопленного опыта. Реализация подхода позволяет существенно уменьшить трудоемкость процесса оценки и повысить обоснованность принимаемых решений.

Введение

Испытание объектов информационных технологий (ОИТ) является сложным наукоемким процессом, реализация которого требует знания исследуемого ОИТ, его уязвимых мест и порождаемых ими проблем информационной безопасности [1]. Международным стандартом ISO/IEC 18045 [2] определена Общая методология испытания продуктов и систем информационных технологий на соответствие различным уровням гарантии оценки (УГО). Для каждого УГО регламентируется совокупность единиц работы, которые в соответствии с требованиями компонентов гарантии из СТБ 34.101.3 (ISO/IEC 15408 «Общие критерии» (ОК)) [3] должны быть выполнены экспертом в процессе оценки безопасности ОИТ. В соответствии с ОК однотипные единицы работы объединяются в подоперации, отвечающие компонентам гарантийных требований, а подоперации – в операции, отвечающие классам гарантийных требований.

Согласно Общей методологии оценка любого объекта должна проводиться в рамках специально разработанной для него схемы оценки (рабочей методики), удовлетворяющей ISO/IEC 18045 и учитывающей специфику объекта. Методика разрабатывается и утверждается в процессе испытания объекта. Процедура ее разработки и реализации в стандарте не регламентируется, однако для повышения объективности оценки декларируется необходимость руководствоваться такими универсальными принципами, как соответствие, беспристрастность, объективность, повторяемость и воспроизводимость, правдоподобие, рентабельность, адаптируемость. Однако на практике эти принципы часто нарушаются, вследствие чего разрабатываемые рабочие методики не удовлетворяют требуемому качеству, что обусловливает невозможность адекватной оценки безопасности ОИТ. Еще одна проблема состоит в том, что в соответствии с ISO/IEC 18045 эксперт должен учесть очень большое количество факторов, разных по своей значимости и не поддающихся четкой количественной оценке, а эффективные методы обработки получаемых массивов экспертных оценок отсутствуют. Кроме того, как показал опыт, недостатком существующего подхода является использование слишком грубой двухбалльной системы оценки, когда относительно каждой единицы работы и ОИТ в целом могут выноситься только два типа заключений: «соответствует», «не соответствует» (без учета значимости обнаруженных недостатков).

Указанные проблемы приводят к неприемлемо большому влиянию субъективного фактора, значительному увеличению трудозатрат и в целом негативно влияют на качество заключения о результатах оценки. Для преодоления данных недостатков естественно по возможности формализовать и автоматизировать процесс оценки [4]. С этой целью в статье предлагается подход, основанный:

– на формировании баз знаний, характеризующих единицы работы, которые регламентированы стандартом ISO/IEC 18045 для разных уровней гарантии оценки – УГО1–УГО4;

– формировании баз знаний, аккумулирующих накопленный опыт и содержащих практические рекомендации по проведению оценки, в том числе в части тестирования разных типов уязвимостей и ОИТ;

– введении более гибкой пятибалльной шкалы оценки (вместо двухбалльной системы оценки);

– ранжировании единиц работы по их значимости для оценки безопасности ОИТ;

– автоматизации процесса оценки, в том числе процесса обработки больших массивов экспертных оценок на основе перехода от качественных к количественным оценкам, и использовании методов нечеткой формализации, позволяющих учесть субъективность и неопределенность исходных данных.

1. Общая методология оценки безопасности ОИТ

В соответствии с действующей международной и национальной нормативно-методической базой [2, 3] общая методология оценки безопасности ОИТ состоит в следующем: оценка ОИТ проводится в организации, аккредитованной в качестве испытательной лаборатории или испытательного центра, в проведении оценки принимают участие специалисты испытательной лаборатории (испытательного центра), разработчик ОИТ, разработчик тестов, а при необходимости и заказчик или потребитель ОИТ.

Испытание ОИТ предполагает проведение предварительной оценки задания по безопасности (ЗБ), разработанного в соответствии с ОК. Если эксперт вынес заключение о пригодности ЗБ, то испытание ОИТ состоит в оценке полноты реализации комплексом средств безопасности объекта (КСБО) совокупности функциональных требований безопасности (ФТБ), сформулированных в ЗБ, и осуществляется в соответствии с УГО, заявленным в ЗБ.

Продолжительность испытания зависит от архитектуры и состава ОИТ, а также от УГО, на соответствие которому производится оценка. Исходные данные, которые должен предоставить разработчик, определяются в стандарте ISO/IEC 18045 и зависят от УГО. Если ОИТ ранее подвергался оценке, то должны быть представлены результаты предыдущих оценок.

Процесс испытания регламентируется рабочей методикой и сводится к выполнению большой совокупности проверок различных требований безопасности к ОИТ. Каждая проверка завершается вынесением соответствующей экспертной оценки, по совокупности которых формируется общее заключение (вердикт) эксперта о защищенности ОИТ.

Для поддержки соответствия рабочих методик стандартам нужно обеспечить прямое соответствие между структурой требований безопасности ОК (класс, семейство, компонент и элемент) и структурой действий в процессе испытаний (операция, подоперация, действие, единица работы). Понятие «операция» относится к классу гарантийных требований безопасности (ГТБ). Понятие «подоперация» относится к компоненту ГТБ. Семейства ГТБ явно не применяются при оценке, так как оценка проводится по единственному компоненту из семейства. Термин «действие» относится к элементу действия эксперта в соответствии с ОК. Различают действия по проверке требований к содержанию и представлению доказательств и действия по проверке требований, реализованных разработчиком. Единица работы описывает самый нижний уровень работы эксперта при оценке. Каждое действие включает одну или более единиц работы. Любая единица работы, не вытекающая напрямую из требований ОК, выражается в терминах задач и подзадач.

2. Постановка задачи

Примем следующие обозначения:

T – подлежащий оценке ОИТ;

$Z(T)$ – предварительно оцененное ЗБ для ОИТ T;

L, $1 \le L \le 4$, – уровень гарантии, на соответствие которому требуется оценить ОИТ T;

$W_L = \{w_{1L}, \ldots, w_{D(L)}\}$ – совокупность единиц работы, подлежащих выполнению в ходе оценки ОИТ T по УГО L в соответствии с ОК и ISO/IEC 18045 (для любого L значение $D(L)$ достаточно велико);

$E = \{e_1, \ldots, e_M\}$ – множество экспертов, участвующих в оценке ОИТ T;

O – лингвистическая шкала, используемая для формирования экспертных оценок;

$A_n = \{ a_n^1, \ldots, a_n^{D(L)} \}$ – множество лингвистических оценок по единицам работ W_L, которые в соответствии со шкалой O выставлены экспертом e_n, $1 \le n \le M$, в ходе оценки ОИТ T.

Обозначим через $I_n(T)$ интегральную оценку ОИТ T на соответствие ЗБ $Z(T)$, выставленную экспертом e_n, и через $I(T) \in O$ – коллегиальную интегральную оценку коллектива экспертов E, формируемую на основе совокупности оценок $\{I_n(T) \mid I_n(T) \in O, 1 \le n \le M\}$.

Ставится задача: по совокупности оценок $A_1,\ldots,A_M$ получить оценку $I(T) \in O$. Основными критериями эффективного решения данной задачи являются качество (адекватность) формируемой оценки $I(T)$ и трудоемкость ее выполнения.

3. Общая схема подхода

Предлагаемый подход включает несколько этапов:

1. Для поддержки процесса испытания ОИТ формируется ряд баз знаний:

– четыре базы знаний, содержащие описание регламентных единиц работы по оценке ОИТ на соответствие УГО1–УГО4. Базы знаний формируются согласно ISO/IEC 18045. Для каждой единицы работы приводятся ее описание, практические рекомендации по проведению оценки, балльная шкала оценки и вес, позволяющий ранжировать единицы работы по степени их относительной важности при оценке безопасности. Определяются также веса подопераций и операций;

– базы знаний, аккумулирующие опыт испытания разных типов ОИТ. Для каждого типового ОИТ приводятся описание потенциальных уязвимых мест; примерный вопросник эксперта разработчику; описание тестов, продемонстрировавших свою эффективность при предыдущих испытаниях объектов данного типа; прочие рекомендации по проведению испытаний.

2. Осуществляется предварительное рассмотрение предоставленных заказчиком материалов с целью определения возможности приемки ОИТ к испытанию. После необходимых согласований с заказчиком и приемки ОИТ к испытанию производится переход к непосредственному процессу оценки.

3. Разрабатывается рабочая методика оценки. Эксперты выбирают базу знаний того УГО, на соответствие которому испытывается ОИТ, и определяют (в соответствии с ЗБ и спецификой ОИТ) перечень операций, подопераций и единиц работы, подлежащих проверке. Формулировки единиц работы уточняются с учетом специфики ОИТ, а рекомендации по их выполнению дополняются конкретными практическими рекомендациями, отражающими опыт испытания ОИТ данного типа. Для указанной адаптации можно использовать базу знаний, содержащую опыт испытания ОИТ соответствующего типа.

Для каждой единицы работы, подоперации и операции проводится (с учетом специфики ОИТ и требований заказчика) необходимая корректировка заданных по умолчанию весов и шкал оценки. В подходе по умолчанию определяются две комбинированные шкалы оценки (для ранжирования единиц работы, подопераций, операций и для оценки степени соответствия ОИТ требованиям ЗБ на уровне единиц работы, подопераций, операций и объекта в целом). Шкалы включают перечень допустимых лингвистических оценок и соответствующие им интервалы количественных оценок.

Разработанная рабочая методика передается на согласование в орган, заказывающий проведение оценки.

4. Проводится испытание ОИТ в соответствии с рабочей методикой. Эксперт выполняет включенные в нее единицы работы с учетом приведенных рекомендаций. По результатам выполнения единицы работы выставляется оценка, отражающая степень выполнения соответствующего требования безопасности. С использованием заданной комбинированной шкалы эксперт выставляет лингвистическую оценку [5] и затем уточняет ее количественно в рамках соответствующего числового интервала.

5. На основании совокупности оценок единиц работы, полученных на этапе 4, определяется совокупность количественных оценок для подопераций и операций, а затем – количественная интегральная оценка информационной безопасности ОИТ. Для определения оценок используются взвешенные аддитивные свертки.

6. На основании количественной интегральной оценки, полученной на этапе 5, определяется лингвистическая интегральная оценка, которая принимается в качестве итогового заклю-

чения эксперта об информационной безопасности ОИТ. Для определения лингвистической оценки используются методы интервального анализа [6].

7. На основе совокупности заключений экспертов определяется общая коллегиальная оценка защищенности ОИТ.

8. Формируется технический отчет по результатам оценки и протокол испытаний (оценки).

9. База знаний, описывающая опыт испытания ОИТ, пополняется результатами выполненной оценки.

4. Шкалы оценки

Как показывает опыт, для проведения оценки обычно можно использовать одну общую шкалу оценки единиц работы, подопераций, операций и в целом ОИТ и одну общую шкалу ранжирования единиц работы, подопераций и операций. Ниже предлагаются две возможные шкалы, которые могут корректироваться экспертами (при возможном участии заказчика) с учетом специфики испытываемого ОИТ.

4.1. Шкала оценки качества операций, подопераций и единиц работы

Как отмечается в [5], при экспертной оценке свойств объектов, как правило, целесообразно использовать шкалы, имеющие пять-семь градаций. С учетом накопленного опыта предлагается применять следующую лингвистическую шкалу оценки безопасности ОИТ:

а) «строгое соответствие» – ОИТ полностью соответствует требованиям ЗБ и пригоден для безопасного использования без всяких изменений;

б) «высокая степень соответствия» – существенные замечания относительно безопасности ОИТ отсутствуют и он пригоден для использования с учетом рекомендаций экспертов;

в) «средняя степень соответствия» – ОИТ содержит незначительные недостатки, которые тем не менее приводят к нарушению соответствия требованиям ОК, и требует соответствующей доработки;

г) «низкая степень соответствия» – ОИТ содержит отдельные существенные недостатки, которые приводят к значительному нарушению соответствия требованиям ЗБ, и требует соответствующей переработки;

д) «несоответствие» – ОИТ не соответствует требованиям ЗБ и не пригоден для использования.

В случае заключений б) – д) эксперт должен предоставить описание существующих проблем, оценку их серьезности, указать организации, ответственные за решение проблем, рекомендуемые сроки их решения, влияние проблем на экспертное заключение.

Эксперт может также сделать заключение «оценка не завершена», если он по каким-либо причинам не смог выполнить оценку ОИТ в полном объеме. При этом он должен указать причины, не позволившие произвести полную оценку.

Для оценки единиц работы, операций, подопераций также используется приведенная выше лингвистическая шкала оценок, формируемых в соответствии с критериями, аналогичными а) – д).

Исходя из накопленного опыта оценки, по умолчанию можно использовать одну и ту же таблицу соответствия лингвистической и интервальной шкал (например, представленную в табл. 1).

Таблица 1

Соответствие между лингвистической и интервальной шкалами оценок

Лингвистическая оценка степени соответствия	Интервал количественных оценок
Строгое соответствие	1,0–0,8
Высокая степень соответствия	0,79–0,6
Средняя степень соответствия	0,59–0,4
Низкая степень соответствия	0,39–0,2
Несоответствие	0,19–0,01

Предлагается использовать следующую комбинированную шкалу оценки (рис. 1), которая каждому значению лингвистической шкалы сопоставляет числовой интервал значений для уточнения степени соответствия оцениваемого свойства ОИТ выбранному уровню. Положение движка слайдера относительно границ интервала характеризует степень уверенности эксперта в выполнении оцениваемого требования на соответствующем уровне.

Рис. 1. Макет комбинированной шкалы оценки

4.2. Шкала оценки важности операций, подопераций и единиц работы

В процессе оценки необходимо учитывать, что единицы работы, подоперации и операции не являются равнозначными (с точки зрения оценки безопасности ОИТ) и вследствие этого они должны быть проранжированы.

Представляется целесообразным использовать, например, следующую единую лингвистическую шкалу оценки относительной важности единиц работы, подопераций и операций: P = {«весьма важная», «важная», «средней важности», «наименее важная»}.

Исходя из накопленного опыта оценки, по умолчанию для ранжирования единиц работы, подопераций и операций можно использовать единую таблицу соответствия лингвистической и интервальной шкал (например, табл. 2).

Таблица 2

Соответствие между лингвистической и интервальной шкалами важности (веса)

Лингвистическая оценка важности	Интервал количественных оценок
Весьма важная	0,75–1,0
Важная	0,5–0,74
Средней важности	0,25–0,49
Наименее важная	0,01–0,24

5. Метод формирования интегральной оценки

Примем следующие обозначения:

b_n^i – количественная оценка по единице работы w_i, $1 \le i \le D(L)$, сформированная на основе лингвистической оценки $a_n^i \in O$ и выставленная экспертом n, $1 \le n \le M$, в соответствии с табл. 1;

$p(w_i)$ – вес единицы работы w_i, $1 \le i \le D(L)$, установленный для ОИТ T в рабочей методике;

p_i – вес подоперации i, установленный для ОИТ T в рабочей методике;

P^i – вес операции i, установленный для ОИТ T в рабочей методике.

Можно выделить следующие этапы формирования оценки:

– экспертная оценка безопасности ОИТ в соответствии с регламентированными единицами работы, определение совокупности оценок $\{b_n^i, i = 1,\ldots,D(L), n = 1,..,M\}$;

– обработка экспертных данных каждого эксперта и получение совокупности интегральных оценок $\{I_n(T) \in O, n=1,...,M\}$;

– определение интегральной оценки документа $I(T) \in O$ как общего заключения коллектива экспертов.

Обработка результатов работы каждого эксперта e_n, $1 \le n \le M$, включает, в свою очередь, следующие шаги:

– формирование количественных оценок подопераций;

– формирование количественных оценок операций;
– формирование количественных оценок безопасности ОИТ T по УГО L;
– вычисление лингвистической интегральной оценки $I_n(T)$ безопасности ОИТ T экспертом.

5.1. Определение интегральной оценки ОИТ одним экспертом

Одним из возможных подходов к получению обобщенных оценок показателей качества является использование взвешенных аддитивных сверток.

Для вычисления оценки o_n^j j-й подоперации экспертом e_n может использоваться формула

$$o_n^j = \frac{\sum_{k=1}^{t_j} p(w_{j(k)}) \cdot b_n^{j(k)}}{\sum_{k=1}^{t_j} p(w_{j(k)})},$$

где $\{w_{j(1)},\ldots,w_{j(t_j)}\}$ – множество регламентированных единиц работы, связанных с оценкой по j-й подоперации.

В соответствии с табл. 1 все количественные оценки вида $b_n^{j(k)}$ удовлетворяют неравенству $b_n^{j(k)} \le 1$. Отсюда следует, что все показатели качества вида o_n^j также удовлетворяют неравенству $o_n^j \le 1$.

Оценка Q_n^g g-й операции экспертом e_n может вычисляться по формуле

$$Q_n^g = \frac{\sum_{k=1}^{v_g} p_k \cdot o_n^k}{\sum_{k=1}^{v_g} p_k},$$

где $\{o_n^1,\ldots,o_n^{v_g}\}$ – множество регламентированных подопераций, связанных с оценкой по g-й операции.

Из условия $o_n^j \le 1$, $\forall\ j = 1,\ldots,v_g,$ следует, что все показатели качества вида Q_n^g также удовлетворяют неравенству $Q_n^g \le 1$.

Оценка $o_n(T)$ степени соответствия ОИТ T ЗБ, разработанного по требованиям УГО L, экспертом e_n может вычисляться по формуле

$$o_n(T) = \frac{\sum_{g=1}^{R(L)} P^g \cdot Q_n^g}{\sum_{g=1}^{R(L)} P^g},$$

где $\{Q_n^1, \ldots, Q_n^{R(L)}\}$ – множество регламентированных операций, связанных с оценкой ОИТ по УГО L.

Из условия $Q_n^g \le 1$, $\forall\ g = 1,\ldots,R(L)$, следует, что оценка $o_n(T)$ удовлетворяет условию $o_n(T) \le 1$.

Для вынесения заключения о соответствии ОИТ УГО L требуется правило перевода сформированной количественной оценки $o_n(T)$ в лингвистическую переменную $I_n(T) \in O$. Для этого можно использовать методы интервальной оценки [6].

При условии, что e_n выполнил все регламентированные единицы работы, для формирования заключения $I_n(T)$ можно использовать следующее решающее правило:

– если $o_n(T) \geq \delta_1$, то $I_n(T) = O_1$ (строгое соответствие);

– если $\delta_2 \leq o_n(T) < \delta_1$, то $I_n(T) = O_2$ (высокий уровень соответствия);

– если $\delta_3 \leq o_n(T) < \delta_2$, то $I_n(T) = O_3$ (средний уровень соответствия);

– если $\delta_4 \leq o_n(T) < \delta_3$, то $I_n(T) = O_4$ (низкий уровень соответствия);

– если $o_n(T) < \delta_4$, то $I_n(T) = O_5$ (несоответствие).

Здесь $1 > \delta_1 > \delta_2 > \delta_3 > \delta_4 > 0$ – заданные пороговые значения, определяемые коллективом экспертов с участием заказчика.

5.2. Определение общей интегральной оценки ОИТ коллективом экспертов

Процедура определения коллективного заключения об информационной безопасности ОИТ разбивается на два основных этапа: проверка согласованности мнений экспертов и определение общей интегральной оценки $I(T) \in O$.

Проверка степени согласованности мнений экспертов. Проверка согласованности мнений экспертов может основываться на оценке отличия мнения каждого отдельного эксперта e_n, $1 \leq n \leq M$, от мнения коллектива экспертов в целом. Рассмотрим возможную процедуру оценки.

Пусть $\overline{O_k}$, $1 \leq k \leq D(L)$, – средняя количественная оценка единицы работы w_k коллективом экспертов $e_1,\ldots,e_M$ с учетом их квалификации: $\overline{O_k} = \frac{1}{M}\sum_{n=1}^{M} \nu(n) \cdot b_n^k$, где $\nu(n)$ – оценка квалификации эксперта e_n. Определение $\nu(n)$, n=1,…,M, возлагается на руководителя испытаний. Мера σ_n отклонения оценок эксперта e_n может вычисляться по формуле

$$\sigma_n = \frac{\sum_{k=1}^{D(L)} p(w_k) \cdot \left| b_n^k - \overline{O}_k \right|}{\sum_{k=1}^{D(L)} p(w_k)}.$$

Пусть δ^* – заданное пороговое значение отклонения, определяемое руководителем коллектива экспертов. Критерием согласованности оценок коллектива экспертов является выполнение условия

$$\sigma_n \leq \delta^*, \ \forall\ n = 1,\ldots,M.$$

Нетрудно видеть, что из условия $b_n^k \leq 1,\ \forall k = 1,...,D(L),\ \forall n = 1,...,M$, следует неравенство $\sigma_n \leq 1$, а из него $\delta^* \in [0,1)$. Если для эксперта e_n, $1 \leq n \leq M$, выполняется условие $\sigma_n > \delta^*$, то принимается решение о неприемлемо большом отклонении его оценки от оценок остальных экспертов. По отношению к каждому из таких экспертов могут быть выбраны, например, следующие стратегии:

– предложить дать обоснование своих результатов оценки;

– провести совместное обсуждение результатов оценки эксперта и принять одно из следующих решений: исключить эксперта из состава группы, обязать эксперта провести повторную оценку, принять мнение эксперта в качестве основного.

Указанный процесс согласования должен продолжаться до тех пор, пока не будет выполнено условие (2).

Определение общей интегральной оценки. Общая интегральная оценка $I(T) \in O$ определяется после обеспечения выполнения условия $\sigma_n \leq \delta^*$, $\forall\ n = 1,\ldots,M$. Выбор общего заключения $I(T)$ может осуществляться по одному из следующих принципов:

простого большинства – принимается заключение, которое сделало большинство экспертов;

квалифицированного большинства – принимается заключение, которое сделало большинство экспертов, при условии, что их число превышает заданное пороговое значение $\delta_{I(T)}$, определяемое с участием заказчика.

5.3. Определение весов

Важной задачей, возникающей в рамках предложенного подхода, является задача определения весов единиц работы, подопераций и операций. Ввиду того что целью статьи является общее описание подхода к оценке ОИТ, ниже приводится лишь возможная общая схема ее решения. Определение весов разбивается на два основных этапа:

– определение весов отдельными экспертами;

– выработка весов коллективом экспертов.

Определение весов экспертом. Каждый эксперт самостоятельно определяет совокупность весов единиц работы, подопераций и операций. Для этого может использоваться, например, следующая простейшая процедура:

– эксперт e_n последовательно просматривает все подлежащие оценке подоперации;

– в рамках каждой подоперации j эксперт рассматривает совокупность подлежащих оценке единиц работы $\{w_{nj(1)},\ldots,w_{nj(t_j)}\}$ и выполняет следующие действия: выбирает наиболее важную, по его мнению, единицу работы $w^*_{nj(1)}$, присваивает ей наивысший ранг и исключает из дальнейшего рассмотрения, на множестве $\{w_{nj(1)},\ldots,w_{nj(t_j)}\}\backslash\{w^*_{nj(1)}\}$ оставшихся единиц работы снова выбирает наиболее важную единицу работы $w^*_{nj(2)}$, присваивает ей следующий по значимости ранг и т. д. Данная процедура продолжается до тех пор, пока не будут упорядочены по значимости все единицы работы;

– в рамках каждой подоперации j-й эксперт присваивает единицам работы веса $p(w^*_{nj(1)}),\ldots,p(w^*_{nj(t_j)})$. При определении весов эксперт использует комбинированную шкалу весов (аналогичную шкале оценки, приведенной на рис. 1), выставляя лингвистическую оценку веса и уточняя ее с помощью движка слайдера относительно границ интервала в соответствии со степенью его уверенности в оценке. При этом должно быть обеспечено выполнение условия $p(w^*_{nj(1)})>\ldots>p(w^*_{nj(t_j)})$ в соответствии с упорядоченностью $w^*_{nj(1)},\ldots,w^*_{nj(t_j)}$;

– эксперт последовательно просматривает все подлежащие оценке операции и по аналогии с приведенной выше процедурой определяет веса подопераций и операций.

Для облегчения работы эксперта и уменьшения субъективного фактора предлагается использовать базу знаний, аккумулирующую накопленный опыт. Она включает известные результаты из различных доступных источников и связана с решением следующих задач:

– определение групп однотипных (с точки зрения существующих проблем безопасности) продуктов и систем информационных технологий (классификация ОИТ). В качестве критериев классификации выступают тип ОИТ, конфигурация ОИТ, среда эксплуатации и т. д.;

– определение для каждого класса ОИТ эталонных цепочек (для разных УГО) упорядоченности единиц работы, подопераций и операций по их значимости с учетом специфики класса объектов;

– описание положительного опыта в части определения весов для разных классов ОИТ;

– вопросники, содержащие примерный перечень вопросов для разных классов ОИТ, которые эксперту целесообразно задать заказчику (разработчику) для уточнения предлагаемых из опыта весов.

Данная база знаний может использоваться экспертами на основе определения класса ОИТ, соответствующего оцениваемому ОИТ, и применения содержащихся в нем сведений с возможным дальнейшим их уточнением в соответствии со спецификой ОИТ.

Выработка весов коллективом экспертов. Руководитель испытаний обеспечивает выработку общих весов $p(w_i)$, p_i, P^i, $1 \le i \le D(L)$, коллективом экспертов. Для этого может использоваться следующая общая схема:

– проведение ранжирования экспертов по их квалификации;

– вычисление взвешенных (с учетом квалификации экспертов) средних количественных оценок единиц работы, подопераций и операций коллективом экспертов;

– определение степени согласованности весов единиц работы, подоперации и операций, выставленных разными экспертами; устранение неприемлемо больших разногласий (в случае их наличия) на основе проведения совещания экспертов;

– выработка коллективного решения, например с использованием решающего правила типа квалифицированного большинства.

Для реализации указанной схемы можно использовать, например, подход, аналогичный приведенному в разд. 5.2.

6. Подсистема поддержки тестирования

Среди действий по оценке, регламентированных в УГО1–УГО4, целесообразно выделить деятельность по тестированию. Это обусловлено тем, что тестирование, в силу своей сложности и плохой формализуемости, является наиболее проблематичным этапом оценки. Тестирование рассматривается как вид деятельности, целью которой является вынесение заключения о том, ведет ли себя КСБО в соответствии с проектной документацией и ФТБ, идентифицированными в ЗБ. Это достигается путем вынесения экспертного заключения о качестве тестирования КСБО разработчиком на основе выборочного проверочного тестирования предоставленных им материалов и проведения экспертом (в случае необходимости) дополнительного независимого тестирования некоторого подмножества КСБО.

Независимое тестирование трактуется как тестирование на проникновение (преодоление защиты), заключающееся в санкционированной попытке обойти существующий КСБО. При этом эксперт играет роль злоумышленника, мотивированного на нарушение информационной безопасности ОИТ. Для проведения тестирования необходимо определить состав и структуру репрезентативной выборки тестов с учетом идентифицированных уязвимых мест. Основными критериями при формировании выборки тестов являются полнота, неизбыточность, практическая реализуемость (с учетом допустимых затрат). Принятие решения о завершении тестирования базируется на анализе остаточных уязвимостей и оценке остаточных рисков безопасности.

Для оценки риска $R(Y)$ использования нарушителем уязвимости Y можно применить следующую формулу:

$$R(Y) = P_1(Y) \cdot P_2(Y) \cdot P_3(Y) \cdot P_4(Y),$$

где $P_1(Y)$ – вероятность использования уязвимого места Y в предполагаемой среде безопасности ОИТ; $P_2(Y)$ – вероятность реализации нарушителем (в соответствии с имеющейся моделью нарушителя) успешной атаки на основе Y; $P_3(Y)$ – вероятность того, что реализация атаки приведет к существенному (в соответствии с заданными критериями) ущербу; $P_4(Y)$ – вероятность отказа средств защиты ОИТ, связанных с отражением атак, которые используют Y.

В качестве критерия необходимости тестирования уязвимости Y может применяться условие

$$R(Y) \geq \Delta,$$

где Δ – заданный порог критичности, устанавливаемый в рабочей методике оценки исходя из специфики ОИТ и требований безопасности, предъявляемых в ЗБ.

В качестве критерия завершения тестирования может применяться условие

$$R < \Delta^*,$$

где R – средняя взвешенная оценка общего ущерба от нарушения безопасности ОИТ; Δ^* – заданный порог защищенности ОИТ T, устанавливаемый в рабочей методике оценки исходя из специфики ОИТ и требований безопасности, предъявляемых в ЗБ. Значение величины R вычисляется по формуле

$$R = \frac{\sum_{i=1}^{K} p(Y_i) \cdot R(Y_i)}{\sum_{i=1}^{K} p(Y_i)},$$

где K – количество идентифицированных экспертом остаточных уязвимостей; $p_i(Y)$ – вес, отражающий значимость ущерба от реализации Y_i и определяемый в рабочей методике.

Приведенные вопросы оценки рисков и, в частности, вычисление вероятностей составляют отдельную задачу оценки, которую предполагается рассмотреть в дальнейшем.

Для поддержки тестирования целесообразно использовать базу знаний, содержащую опыт тестирования разных типовых ОИТ. Для каждого типового ОИТ в ней должно быть дано его краткое общее описание (границы, функциональное назначение, защищаемые активы, уязвимые места, угрозы и задачи безопасности, имеющиеся средства безопасности). Должны быть учтены все типы уязвимостей: объективные (сопутствующие техническим средствам, аппаратные и программные закладки и т. д.), субъективные (ошибки, нарушения режимов доступа, эксплуатации, конфиденциальности), случайные (сбои, отказы, повреждения). База знаний должна содержать примерный перечень вопросов, которые эксперт может задать разработчику в ходе тестирования (прежде всего относительно слабых мест ОИТ). База знаний должна включать также описание тестов, продемонстрировавших свою эффективность при предыдущих испытаниях объектов данного типа. Для каждого теста описываются связанные с ним средства безопасности, задачи тестирования, сценарий тестирования. Должен быть реализован журнал тестирования, в который заносится информация о дате тестирования, выполняемом тесте, конфигурации объекта, произошедших в ходе тестирования сбоях, прочих аномалиях (помехах), результатах тестирования и т. д.

Замечание. В целом в рамках предлагаемого подхода экспертам требуется задать 15 «настраиваемых» пороговых значений: δ_1, δ_2, δ_3, δ_4, δ^*, $\delta_{I(T)}$, Δ, Δ^* и пороговые значения, определяющие интервалы количественных оценок (табл. 1 и 2). Пороговые значения определяются исходя из специфики ОИТ и на основе анализа существующих для него рисков безопасности. Методы анализа рисков и определения численных значений порогов составляют отдельную задачу и в данной статье не рассматриваются. Отметим также, что при оценке каждого нового ОИТ можно использовать накопленный опыт, в частности сведения о пороговых значениях, показавших свою правомерность при предыдущих оценках. Как показывает практика, чаще всего можно использовать применявшиеся ранее пороговые значения (возможно, с некоторой корректировкой).

7. Практическая реализация подхода

Для реализации приведенного подхода разработан программный комплекс «ОИТ "Безопасность"», дополняющий и развивающий ранее созданные программные средства разработки и оценки профилей защиты и заданий по безопасности [7–9]. Он предназначен для автоматизации процессов испытаний ОИТ на соответствие УГО1 и УГО2. Программы комплекса могут также служить справочным руководством разработчикам ОИТ для получения консультаций относительно требований, предъявляемых к объекту.

Структура информационного обеспечения программы «ОИТ "Безопасность"» изображена на рис. 2. В состав программы входят: страница «Интегральная оценка», страницы оценки для каждой единицы работы, страницы настройки шкалы весов для интегральной оценки операций и подопераций. Результаты оценки каждого эксперта записываются в базу данных системы и восстанавливаются при повторном входе в нее с тем же именем пользователя.

На странице «Интегральная оценка» (рис. 3) сосредоточена вся информация, необходимая эксперту для принятия решения относительно итоговой оценки объекта на соответствие УГО выбранного уровня.

Результаты оценки единиц работы отражены в виде *таблицы оценок единиц работы*, имеющей скроллер, и двух диаграмм. Таблица содержит порядковый номер, наименование (идентификатор) работы, данные о назначенных экспертом весовых коэффициентах и оценках

уровня соответствия. Обобщенная информация о выставленных оценках представлена в виде круговой диаграммы, отражающей количество тех единиц работы, которые еще не оценивались, оценка которых выше заданного порогового значения и оценка которых ниже этого значения. Пороговое значение может быть задано экспертом в этом же диалоговом окне, по умолчанию оно равно 75. Детализированная информация об оценке единиц работы приводится на столбцовой гистограмме, отражающей уровень соответствия единицы работы по ее порядковому номеру.

Имеются также следующие сведения о процессе оценки. Вычисляется среднее значение оценки по всем единицам работы, фиксируется длительность последнего сеанса работы с программой, количество сообщений о проблемах, возникших при оценке объекта. Результаты вычислений приводятся в таблице интегральной оценки. В ней даются наименование операции и подоперации, диапазон порядковых номеров соответствующих единиц работы, имеются ячейки для ввода весов операций или подопераций, а также отображаются результаты вычисления оценок операции и подоперации.

Со страницы «Интегральная оценка» может быть запущена процедура синтеза протокола оценки, возможен доступ к базе данных «Оценки документов», которая содержит информацию о результатах оценок ОИТ, проведенных в данной лаборатории.

Страница «Регистрация» позволяет зарегистрировать новый объект оценки и зарегистрироваться новому эксперту. Информация вносится соответственно в базы данных «Объекты» и «Эксперты». Окно регистрации эксперта и объекта, а также окно тематической структуры базы знаний оценки ОИТ, имеющейся в программе, показаны на рис. 4.

Настройка числовых диапазонов шкал для перевода лингвистической оценки объекта в количественную форму осуществляется на страницах «Шкалы уровня соответствия» и «Шкалы весовых коэффициентов». При этом эксперт может изменять ширину каждого диапазона настраиваемой шкалы (рис. 5).

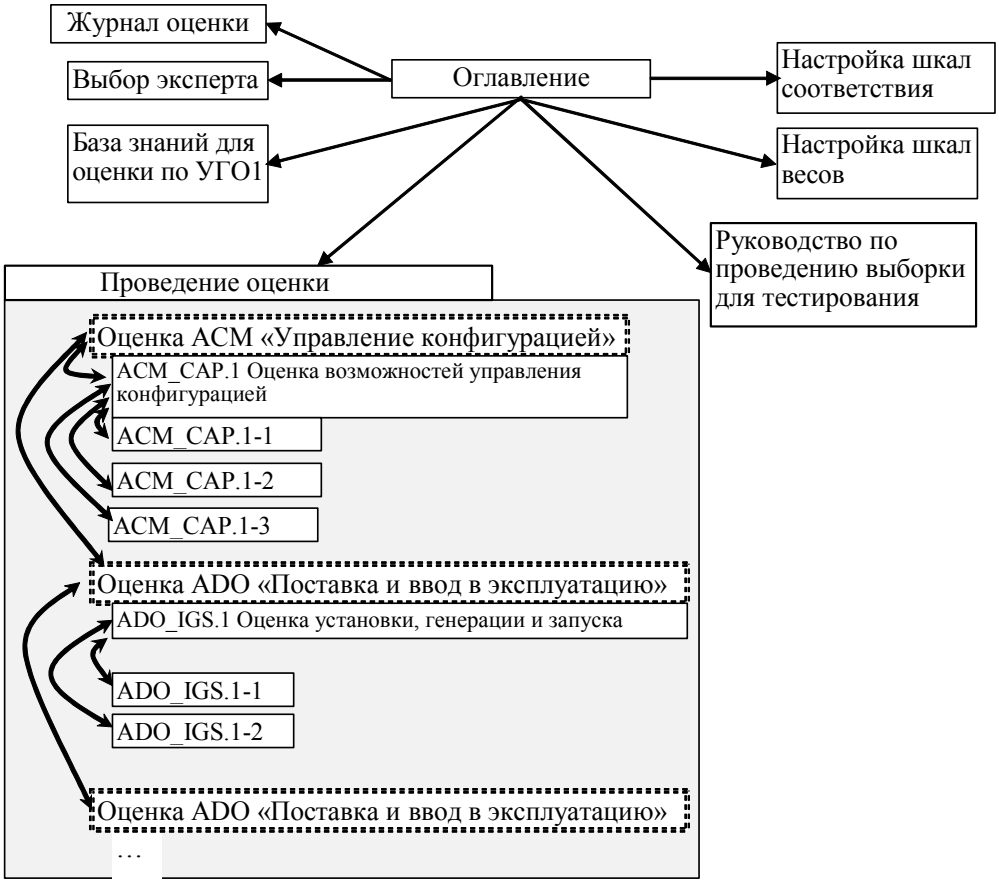

Рис. 2. Структурная схема программы «ОИТ "Безопасность"»

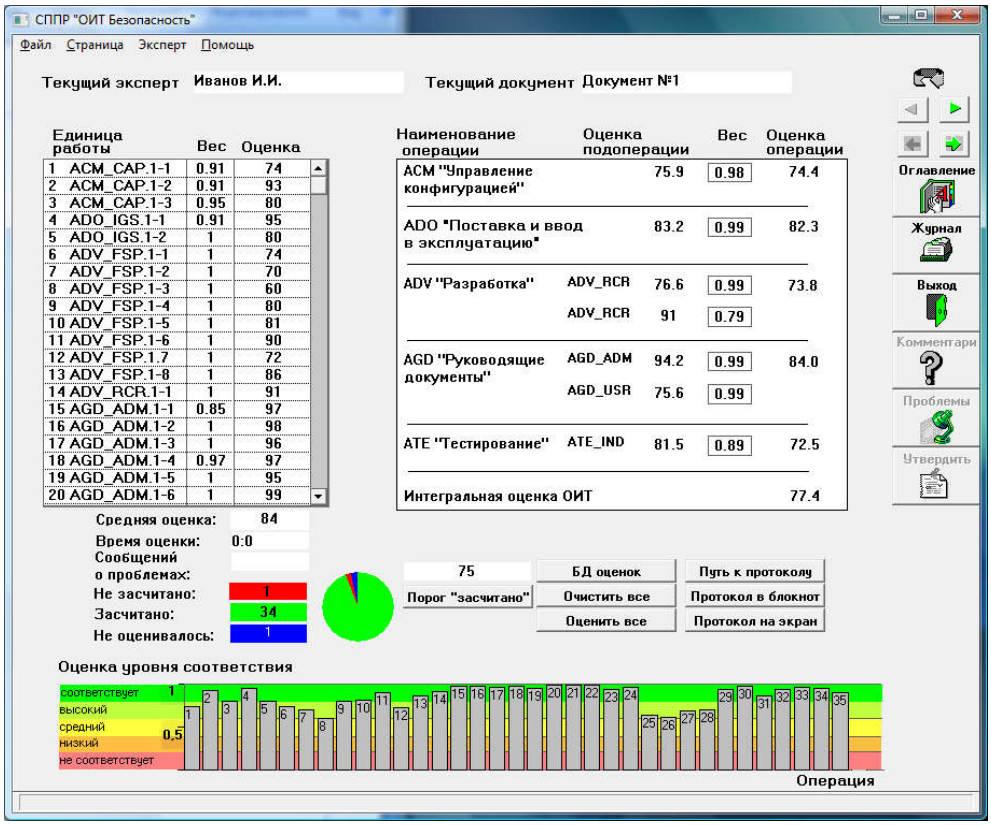

Рис. 3. Вид страницы «Интегральная оценка» программы «ОИТ "Безопасность"»

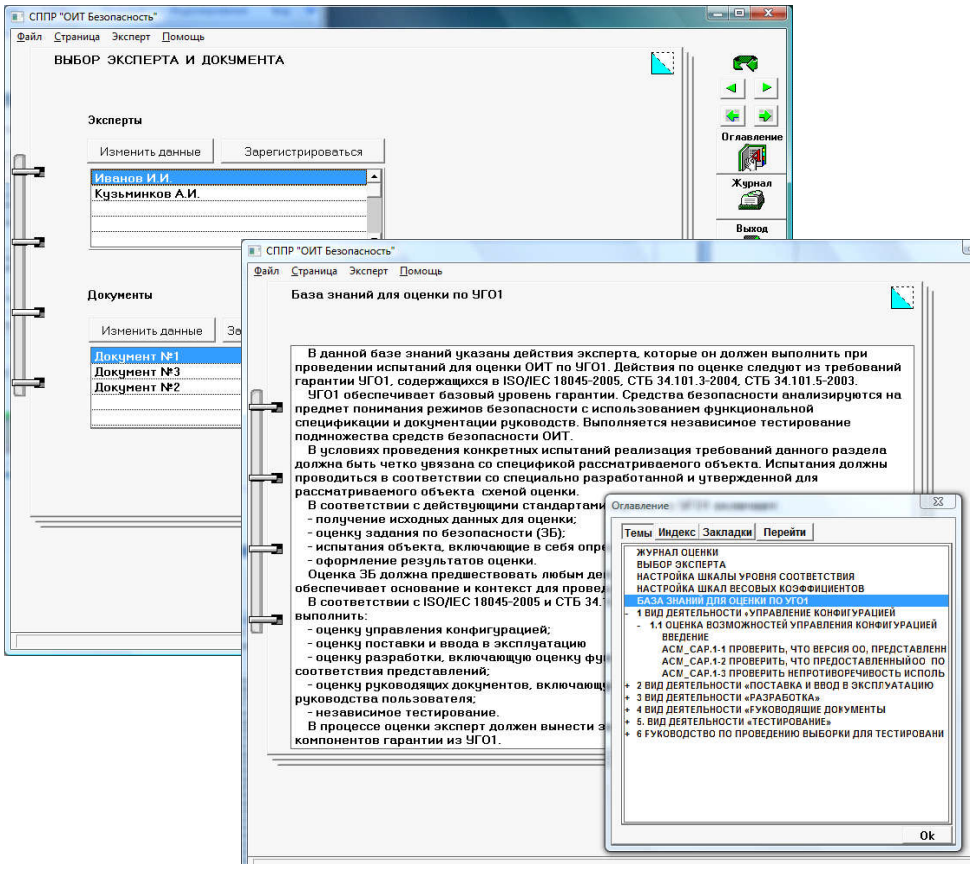

Рис. 4. Тематическая структура программы «ОИТ "Безопасность"»

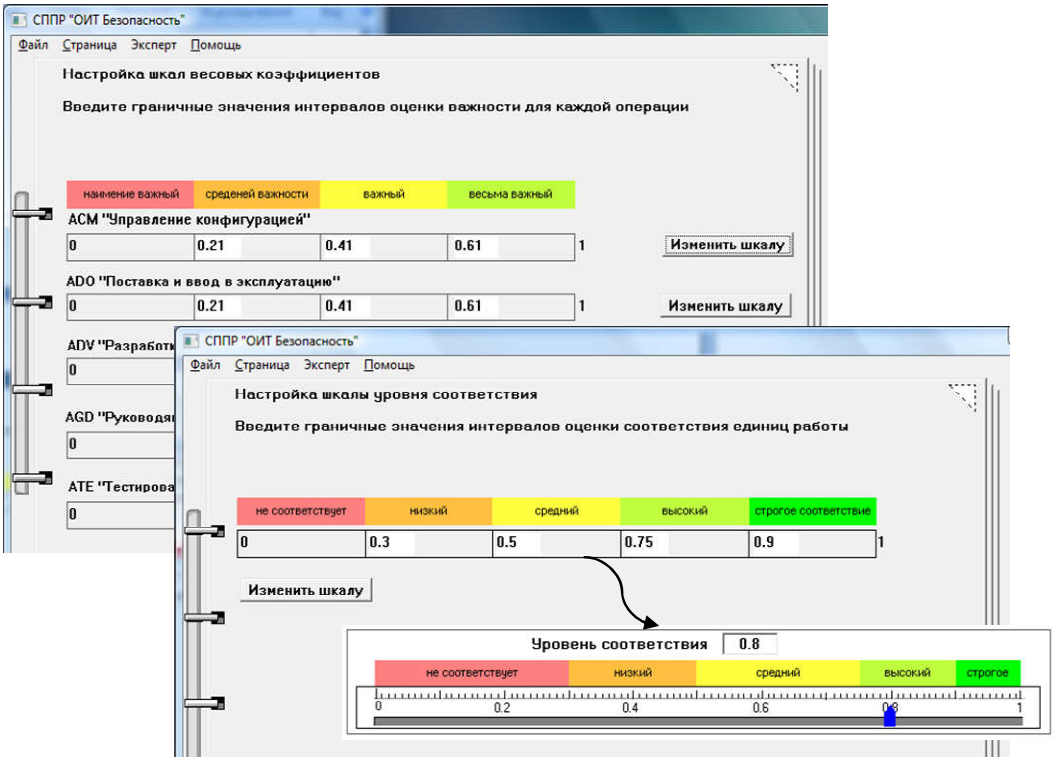

Рис. 5. Настройка диапазонов шкалы уровней соответствия и шкалы весов

На странице оценки операции (рис. 6) эксперт выставляет вес операции, а затем оценку, перемещая мышью указатель на шкале. Есть возможность воспользоваться комментариями относительно особенности проведения оценки по данной операции. Для ввода замечаний о проблемах используется специальная область ввода, для автоматизации ввода имеется список указаний на наиболее часто возникающие проблемы оценки.

По окончании оценки формируется протокол оценки в виде документа Word в формате RTF, который может использоваться как результирующий документ оценки без какой-либо дополнительной обработки.

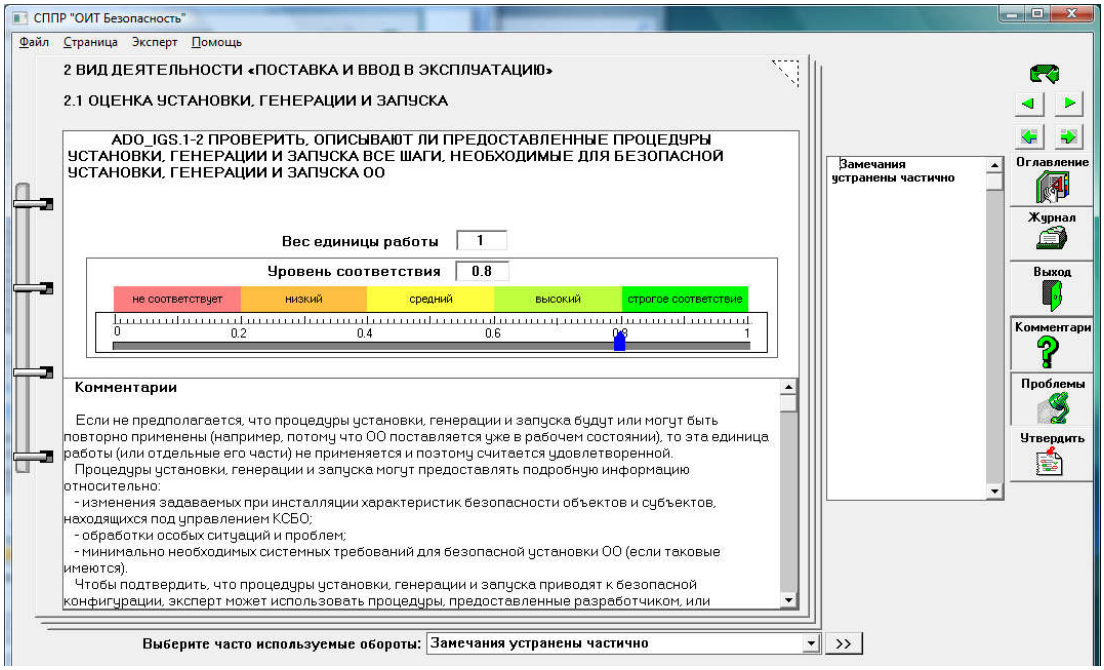

Рис. 6. Страница оценки единицы работы

Программа полностью автоматизирует процесс оценки безопасности объектов информационных технологий, содержит наглядные диаграммы, позволяющие облегчить анализ результатов. Она может быть полезна для разработчиков и заказчиков продуктов и систем информационных технологий, а также для лабораторий, занимающихся испытанием ОИТ.

Заключение

Предложенная методика оценки безопасности ОИТ и основанная на ней автоматизированная система поддержки принятия решения позволит:

– гарантировать соответствие процесса оценки действующим стандартам;

– значительно снизить трудоемкость процесса оценки;

– получить более точные оценки;

– повысить обоснованность результата оценки;

– накапливать и эффективно использовать опыт тестирования разных типов ОИТ.

В настоящей статье не ставилась задача определения пороговых значений используемых показателей качества, хотя такая задача является важной и актуальной. В дальнейшем предполагается разработать методики оценки численных значений порогов на основе оценки рисков, анализа и обобщения опыта предыдущих исследований.

Список литературы

1. Анищенко, В.В. Оценка информационной безопасности / В.В Анищенко // PC Magazine. – 2000. – № 2. – С. 103–108.

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

3. СТБ 34.101.3-2004 (ISO/IEC 15408-3:1999) Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3 : Гарантийные требования безопасности. – Минск : Белорус. гос. ин-т стандартизации и сертификации, 2003. – 112 с.

4. Анищенко, В.В. Об автоматизации процессов оценки безопасности информационных технологий в контексте общих критериев / В.В Анищенко // Комплексная защита информации: сб. науч. тр. – Минск : Ин-т техн. кибернетики НАН Беларуси, 1999. – Вып. 2. – С. 159–168.

5. Заде, Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л.А. Заде. – М. : Мир, 1976. – 165 с.

6. Калмыков, С.А. Методы интервального анализа / С.А. Калмыков, Ю.И. Шокин, З.Х. Юлдашев. – Новосибирск : Наука, 1986. – 221 с.

7. Анищенко, В.В. Требования к автоматизированным средствам разработки профилей защиты / В.В. Анищенко // Управление защитой информации. – 1998. – Т. 2, № 1. – С. 33–36.

8. Анищенко, В.В. Средства автоматизированного формирования функциональных требований безопасности профилей защиты / В.В Анищенко, И.А. Надольский // Управление защитой информации. – 1998. – Т. 2, № 1. – С. 36–38.

9. Максимович, Е.П. Об одном подходе к автоматизации процесса оценки качества профилей защиты и заданий по безопасности / Е.П. Максимович, В.К. Фисенко, М.С. Шибут // Информатика. – 2008. – № 4 (20). – С. 104–115.

Поступила 24.03.09

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: fisenko @ newman.bas-net.by

U.V. Anishchanka, U.K. Fisenko, E.P. Maksimovich, M.S. Shibut

AN APPROACH FOR AUTOMATION OF SECURITY EVALUATION PROCESS OF INFORMATION TECHNOLOGY OBJECTS

A formalized approach for automation of security evaluation process of information technology objects is proposed. The evaluation is performed in accordance with the Common Criteria. The approach is based on fuzzy formalization and expert experience. Implementation of the approach allows substantially reduce the laboriousness of the evaluation process and increase the validity of decisions.