УДК 681.03

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

ОБ ОДНОМ ПОДХОДЕ К АВТОМАТИЗАЦИИ ПРОЦЕССА ОЦЕНКИ КАЧЕСТВА ПРОФИЛЕЙ ЗАЩИТЫ И ЗАДАНИЙ ПО БЕЗОПАСНОСТИ

Предлагается подход к автоматизации процесса оценки качества профилей защиты и заданий по безопасности, соответствующий требованиям Общих критериев и основанный на определении иерархической системы показателей качества и нечеткой формализации. Реализация подхода позволяет существенно уменьшить трудоемкость процесса оценки и повысить обоснованность принимаемых решений.

Введение

Методическими документами, используемыми в Республике Беларусь для оценки качества профилей защиты (ПЗ) и заданий по безопасности (ЗБ), являются международный стандарт ИСО/МЭК 15408–3–1999 (или более поздние версии) и национальные стандарты СТБ 34.101.3–2004, СТБ П 34.101.7–2003 и СТБ П 34.101.6–2003 [1–4]. В соответствии с этими стандартами методический подход к оценке качества ПЗ (ЗБ) состоит в последовательном анализе экспертом разделов документа по обобщенным показателям «полнота», «связность», «непротиворечивость» и вынесении на основании этого заключений о качестве каждого отдельного раздела, а затем и документа в целом. Оценка каждого из показателей раздела основана на экспертной проверке уровня соответствия определенной совокупности регламентированных требований. Результаты оценки представляются в двухбалльной шкале: «соответствует требованиям стандарта», «не соответствует требованиям стандарта». Положительный результат оценки документа в целом («соответствует требованиям стандарта») означает, что ПЗ (ЗБ) пригоден для создания на его основе объекта информационных технологий. В противном случае делается заключение о непригодности документа.

Другие страны также используют для оценки качества ПЗ (ЗБ) ИСО/МЭК 15408–3–1999 (или более поздние версии).

В процессе проведения оценок специалисты-испытатели на опыте убедились, что существующий подход имеет ряд недостатков, наиболее значительные из которых состоят в следующем:

– двухбалльная система оценки («соответствует», «не соответствует») является слишком категоричной и не отражает степени непригодности и возможности доработки документа в случае отрицательного заключения;

– отсутствует четкое описание понятий полноты, связности, непротиворечивости как для отдельных разделов, так и для документа в целом, что затрудняет оценку по этим показателям;

– отсутствуют эффективные методы обработки больших массивов (объемов) экспертных оценок регламентированных требований, что негативно влияет на адекватность формируемых оценок обобщенных показателей качества разделов, интегральных оценок разделов и заключения по документу в целом;

– процедура оценки осуществляется полностью вручную, что требует очень больших трудозатрат.

В указанных условиях приобретают актуальность обеспечение обоснованности результатов оценки и снижение трудоемкости процесса оценки до приемлемого уровня. Основой предлагаемого подхода является опыт, накопленный в процессе проведения оценок документов, представляемых различными организациями. В качестве основных путей решения данных задач специалисты предлагают разработку эффективных методик и методов формирования и обработки массива экспертных оценок и автоматизацию на их основе процесса оценки. В статье предложены пути усовершенствования существующего подхода к оценке ПЗ (ЗБ) за счет определения более гибкой шкалы оценки требований, показателей, разделов и документа в целом; введения иерархической системы

понятий полноты, связности, непротиворечивости для разных структурных составляющих документа; использования формальных методов обработки экспертных данных, основанных на декомпозиции процесса оценки и нечеткой формализации, которая позволяет учесть субъективность и неопределенность исходных данных. Приводятся общая характеристика и архитектура автоматизированной системы поддержки принятия решения, реализующей предлагаемый подход.

1. Иерархическая система показателей качества профилей защиты и заданий по безопасности

В соответствии с работами [1–4] качество структурных составляющих (разделов, подразделов) ПЗ и ЗБ, а также документа в целом оценивается показателями полноты, связности и непротиворечивости. При этом неявно предполагается, что в процессе оценки эксперт должен самостоятельно конкретизировать общие определения показателей в соответствии со спецификой каждого рассматриваемого раздела или подраздела. Такая ситуация оказывает негативное влияние на объективность оценки. В целях устранения данного недостатка предлагается ввести необходимые определения показателей для разделов и подразделов ПЗ и ЗБ. Для этого предлагается выделить две группы разделов: описательного характера и базовые.

К описательным разделам относятся «Введение в описание ПЗ (ЗБ)», «Описание объекта», «Замечание по применению ПЗ» (только для ПЗ), «Требования соответствия ПЗ» (только для ЗБ). Для их оценки можно использовать следующие определения показателей качества на уровне общих текстообразующих категорий научно-технического текста:

полнота – категория достаточности представленной информации в соответствии с требованиями к содержанию, предъявляемыми к разделу; достаточность выразительных или дедуктивных средств для представления необходимой информации в разделе;

связность – категория единства тематического содержания текста, характеризующая степень взаимосвязи частей текста и направленности на решение определенной общей задачи; требует наличия причинно-следственных отношений, строгой логической последовательности изложения и представления информации (каждый последующий элемент вытекает из предыдущего или является следующим звеном в повествовании или рассуждении). Различают локальную связность (связность текста в пределах раздела) и глобальную (связь между разделами, обеспечивающая единство текста как смыслового целого). При оценке по показателю связности целесообразно принять во внимание родственную ей категорию цельности – четко выраженную смысловую замкнутость текста, представление информации в виде законченного целого;

непротиворечивость – категория корректности (правильности, согласованности) представления информации. Различают локальную непротиворечивость (непротиворечивость информации на уровне разделов) и глобальную непротиворечивость (согласованность между разделами документа).

К базовым разделам относятся:

– «Среда безопасности объекта» (подразделы «Угрозы», «Политика безопасности», «Предположения безопасности»);

– «Задачи безопасности» (подразделы «Задачи безопасности для объекта», «Задачи безопасности для среды»);

– «Требования безопасности» (подразделы «Функциональные требования», «Гарантийные требования», «Требования безопасности для среды»);

– «Общая спецификация» (только для ЗБ – подразделы «Комплекс средств безопасности», «Меры гарантии»);

– «Обоснование ПЗ» (для ПЗ – подразделы «Обоснование задач безопасности», «Обоснование требований безопасности») или «Обоснование ЗБ» (для ЗБ – подразделы «Обоснование задач безопасности», «Обоснование требований безопасности», «Обоснование общей спецификации», «Обоснование соответствия ПЗ»).

Показатели качества для базовых структурных составляющих определяются исходя из специфики каждого раздела или подраздела. Например, для множеств угроз и задач безопасности понятия полноты, связности и непротиворечивости могут определяться следующим образом:

Множество угроз безопасности является *полным*, если оно целиком покрывает множество уязвимых мест рассматриваемого продукта или системы, выявленных разработчиком или экспертом и существенных с позиций оценки рисков информационной безопасности.

Множество задач безопасности является *полным*, если оно в полной мере противодействует множеству идентифицированных угроз безопасности и обеспечивает выполнение сформулированных правил политики безопасности и предположений безопасности.

При оценке базовых разделов по показателю полноты следует принять во внимание связанную с ним категорию неизбыточности. Свойство неизбыточности полного множества элементов означает, что оно становится неполным при исключении хотя бы одного из его элементов. Избыточность оценивается с позиций оценки рисков информационной безопасности и ведет к неоправданным дополнительным затратам. Неизбыточное множество угроз не должно содержать угрозы, не относящиеся к объекту; угрозы, которые полностью перекрываются другими угрозами; угрозы, ущерб от реализация которых меньше затрат на обеспечение противодействия им. В неизбыточном множестве задач безопасности решение каждой задачи должно вносить свой (не восполняемый другими задачами) вклад в противодействие как минимум одной угрозе.

Показатель связности для угроз и задач безопасности определяет импликативную связь вида «*если…, то…*». Если сформулирована угроза, то для противодействия ей должна быть сформулирована хотя бы одна задача; если сформулирована задача, то она должна быть направлена на противодействие хотя бы одной угрозе.

Показатель *непротиворечивости* для угроз и задач безопасности определяет согласованность и отсутствие противоречий между множеством угроз и задач.

Показатели качества всего документа вычисляются на основе показателей качества его структурных составляющих и должны отражать степень полноты, связности и непротиворечивости ПЗ (ЗБ). Интегральный показатель качества ПЗ (ЗБ) определяется на основании совокупности показателей его полноты, связности и непротиворечивости и должен отражать степень пригодности документа в соответствии с требованиями стандартов [1–4]. Таким образом, в качестве базиса процесса оценки ПЗ (ЗБ) предлагается использовать иерархическую древовидную систему показателей качества (рис. 1), индуцированную структурой ПЗ (ЗБ).

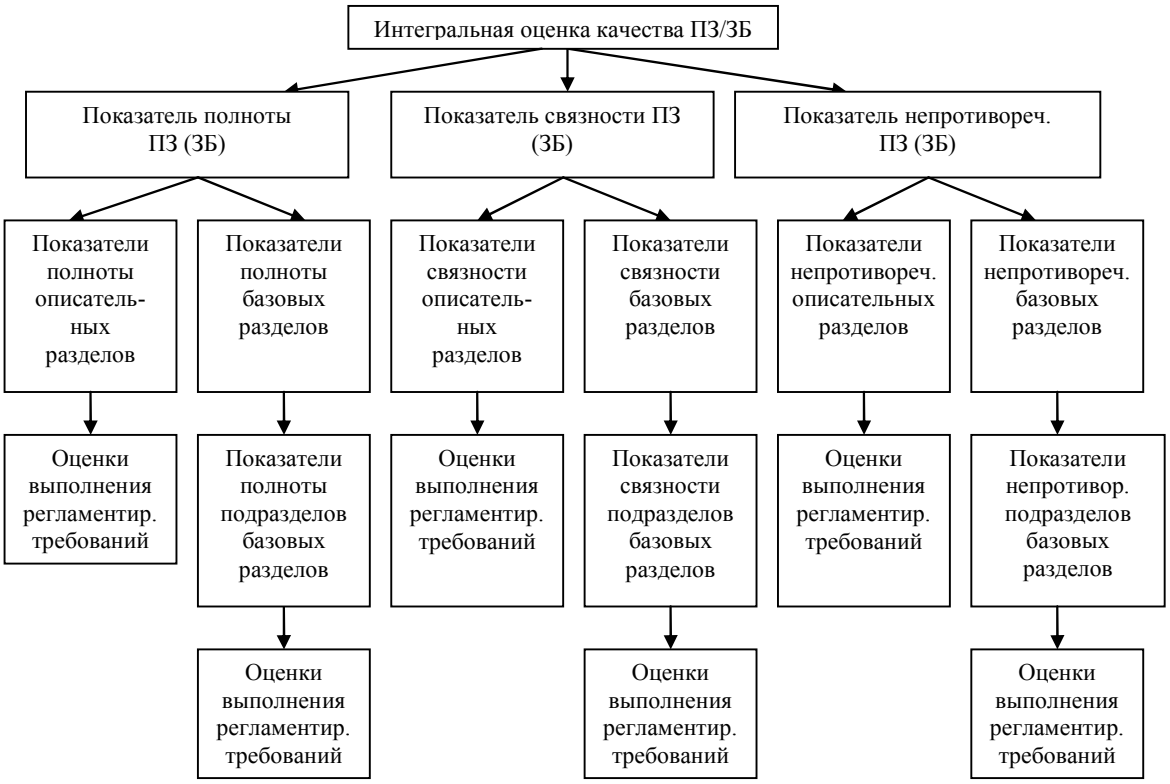

Рис. 1. Иерархическая система показателей качества ПЗ (ЗБ)

Далее для общности изложения будем ссылаться на ПЗ (ЗБ) как на оцениваемый документ, имея в виду, что каждый из этих типов документов имеет свои особенности системы показателей качества в том смысле, что различается количество требований в разделах и коэффициенты важности выполнения этих требований, важности показателей и т. д.

2. Модель процесса оценки качества ПЗ (ЗБ)

Построим модель оценки качества документа с учетом предложенной системы показателей качества. Обозначим через C иерархическую систему показателей полноты, связности, непротиворечивости документа и его структурных составляющих (см. рис.1). Документ, подлежащий оценке, будем обозначать как d, а множество экспертов, участвующих в оценке документа d, – как $E = \{ e_n \mid 1 \le n \le N \}$, где N – количество экспертов, оценивающих документ.

Исходными данными, на основании которых формируется заключение о пригодности документа, являются экспертные оценки уровня его соответствия совокупности регламентированных требований, имеющие качественный характер. Множество требований, подлежащих рассмотрению в ходе оценки документа в соответствии со стандартами СТБ П 34.101.7–2003 и СТБ П 34.101.6–2003, обозначим как $W = \{w_k \mid 1 \le k \le K \}$, где K – общее количество оцениваемых требований (K достаточно велико).

2.1. Шкала оценки качества документа

С целью учета фактора субъективности и неопределенности в оценке указанных требований для формирования оценки предлагается использовать гибкую лингвистическую шкалу, содержащую более двух значений. Обозначим шкалу оценки качества документа как $O = \{O_i \mid i > 2\}$.

В работе [5] отмечается, что при оценке свойств объектов экспертами, как правило, целесообразно использование шкалы, имеющей пять-семь градаций. Исходя из этого и в соответствии с накопленным опытом разработки и оценивания документа предлагается использовать для выставления всех указанных оценок, например, следующую лингвистическую шкалу: O = {«строгое соответствие», «высокий уровень соответствия», «средний уровень соответствия», «низкий уровень соответствия», «несоответствие»}.

В предлагаемой шкале первое значение указывает на полное выполнение рассматриваемого требования (полную пригодность документа); второе, третье и четвертое – на наличие недостатков, требующих доработок документа разной степени; пятое – на полное невыполнение требования, что означает непригодность документа и необходимость разработки вместо него нового документа. Кроме того, эксперт может сделать заключение «оценка не завершена», если он по каким-либо причинам не смог выполнить проверку требования. Если оценка хотя бы одного из регламентированных требований не завершена, то в этом случае задача обработки экспертных данных для оценки документа в целом не возникает, оценка не выставляется. Эксперт в свободной форме указывает причины незавершения работы для последующего внесения в протокол оценки.

Множество лингвистических оценок уровня соответствия документа d требованиям W, выставленных экспертом e_n в ходе проверки, обозначим как $A_n(d) = \{ a_{kn}(d) \mid a_{kn}(d) \in O, 1 \le k \le K\}$, где $a_{kn}(d)$ – лингвистическая оценка степени выполнения требования w_k , выставленная экспертом e_n в ходе проверки документа d, $1 \le n \le N$. На основании лингвистических оценок $a_{kn}(d)$ необходимо определить иерархическую систему показателей качества подразделов и разделов в виде обобщенных оценок – сверток, а также интегральную оценку документа. Ввиду того что экспертные данные являются лингвистическими, определение сверток не представляется возможным без предварительного перевода этих данных в числовую форму представления (количественную шкалу измерения). Для количественной оценки уровня соответствия естественно использовать интервальную шкалу, назначаемую исходя из содержания оцениваемого требования и с учетом специфики документа.

На основании приведенных соображений предлагается использовать комбинированную шкалу оценки (рис. 2), которая каждому значению лингвистической шкалы сопоставляет числовой интервал значений количественной оценки для уточнения степени соответствия оцени-

ваемого свойства документа выбранному уровню. Положение движка слайдера относительно границ интервала характеризует степень уверенности эксперта в выполнении оцениваемого требования на соответствующем уровне.

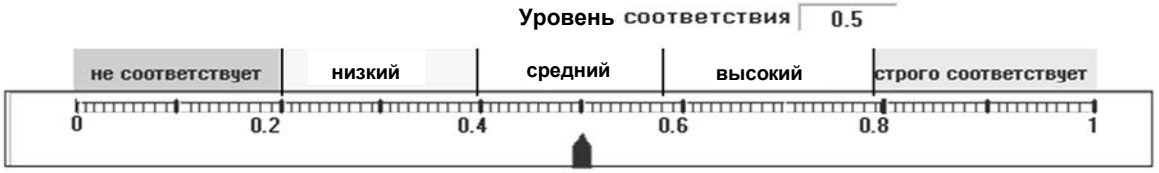

Рис. 2. Макет комбинированной шкалы для выставления оценки соответствия документа отдельному требованию

Обозначим полученную интервальную шкалу оценки документа через $LO = \{(O_i, X_i) \mid O_i \in O, X_i = (x_{i1}, x_{i2}), 1 \le i \le 5\}$, где X_i – интервал числовых значений оценки, соответствующих лингвистической оценке O_i ($x_{i1}, x_{i2} \in [0, 1]$, $x_{i1} < x_{i2}$ и $x_{i1} < x_{j1}$ при $i < j$). Соответственно множество количественных оценок уровня соответствия требованиям w_k, полученных на основе оценок $a_{kn}(d)$, обозначим через $B_n(d) = \{b_{kn}(d) \mid b_{kn}(d) \in [0, 1],\ 1 \le k \le K\}$, где $b_{kn}(d)$ – количественная оценка степени выполнения требования w_k , выставленная экспертом e_n в ходе проверки документа d, $1 \le n \le N$. Каждому требованию может назначаться своя шкала. Априори могут быть заданы допустимые таблицы перевода лингвистических оценок в интервальные, исходя из формулировки требований в нормативных документах. Таблица перевода для дополнительных требований, включенных в документ, рассматривается особо. Исходя из накопленного опыта оценки, по умолчанию для всех требований можно использовать одну и ту же таблицу перевода (например, табл. 1).

2.2. Шкала оценки важности разделов документа и требований к ним

Необходимо также учитывать, что требования, разделы и подразделы не являются равнозначными (с точки зрения оценки качества ПЗ(ЗБ)) и вследствие этого они должны быть проранжированы. С этой целью определим весовые коэффициенты, характеризующие важность разделов документа, показателей качества и отдельных требований: вес описательных и базовых разделов и подразделов; вес каждого показателя качества документа и вес каждого требования, подлежащего проверке экспертом.

Для различных документов веса одних и тех же структурных составляющих могут быть разными. Веса определяются исходя из накопленного экспертами опыта с учетом информации об особенностях конкретного документа, его среде безопасности и решаемых задачах. Назначение весов может осуществляться коллегиально (совместно) всеми экспертами при участии заказчика. При определении весов нужно учитывать следующие обстоятельства:

– необходимость выполнения требования или включения раздела в документ (вес необязательной составляющей обычно меньше веса обязательной);

– вид раздела (веса базовых разделов должны быть больше весов описательных);

– значимость требования или информации, представляемой в подразделе или разделе;

– наличие взаимосвязей между структурными составляющими. Например, базовый раздел может быть непосредственно связан с описательным. Так, вес раздела «Описание объекта» должен зависеть от того, в какой степени представленная в нем информация используется при формулировке угроз безопасности.

Обозначим шкалу оценки важности структурных составляющих документа через $P = \{P_i \mid i > 2\}$. Поскольку при оценке важности структурных составляющих документа не используется значение «не важный», представляется целесообразным использовать, например, следующую лингвистическую шкалу оценки веса: P = {«весьма важный», «важный», «средней важности», «наименее важный»}. Соответствующую интервальную шкалу оценки важности обозначим через $LP = \{(P_i, Y_i) \mid P_i \in P, Y_i = (y_{i1}, y_{i2}), 1 \le i \le 4\}$, где Y_i – интервал числовых значе-

ний оценки, соответствующих лингвистической оценке P_i (y_{i1}, y_{i2} определены аналогично x_{i1} и x_{i2}). Так как важность структурных составляющих обычно оценивается на качественном уровне, необходимо установить таблицу перевода лингвистических оценок важности в количественные. Исходя из накопленного опыта оценки, по умолчанию можно использовать одну и ту же таблицу перевода (например, табл. 2).

Таблица 1

Соответствие между лингвистической и интервальной шкалами оценок

Лингвистическая оценка уровня соответствия	Интервал количественных оценок
Строгое соответствие	0,9–1,0
Высокий уровень соответствия	0,8–0,9
Средний уровень соответствия	0,6–0,8
Низкий уровень соответствия	0,4–0,6
Несоответствие	0,01–0,4

Таблица 2

Соответствие между лингвистической и интервальной шкалами важности (веса)

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

2.3. Постановка задачи оценки качества документа

Пусть, как и ранее:

W – совокупность требований, подлежащих рассмотрению в ходе оценки ПЗ (ЗБ) в соответствии со стандартами СТБ П 34.101.7–2003 (СТБ П 34.101.6–2003);

C – иерархическая система показателей полноты, связности, непротиворечивости ПЗ (ЗБ) и его структурных составляющих;

O – лингвистическая шкала оценки;

d – документ (ПЗ (ЗБ)), подлежащий оценке;

E – множество экспертов, участвующих в оценке документа d;

$A_n(d)$ – множество лингвистических оценок уровня соответствия документа d требованиям из W, которые выставлены экспертом e_n в ходе проверки документа d.

Обозначим через $I(d) \in O$ коллегиальную интегральную оценку качества документа d коллективом экспертов, формируемую на основе совокупности оценок $\{I_n(d) \mid I_n(d) \in O, 1 \le n \le N\}$, где $I_n(d)$ – интегральная оценка документа, выставленная экспертом e_n.

Тогда задача оценки качества документа состоит в следующем. Требуется на основе множеств оценок $A_n(d)$ получить общую коллективную оценку $I(d) \in O$ качества d.

3. Метод формирования интегральной оценки качества ПЗ (ЗБ)

Конкретизируем процедуру формирования интегральной оценки качества документа, основанную на применении стандартов [1–4]. Выделим следующие этапы формирования оценки:

– экспертиза уровня соответствия документа регламентированным требованиям стандарта путем определения оценок вида b_{kn}, где $1 \le k \le K$, $1 \le n \le N$;

– обработка данных каждого с получением интегральной оценки $I_n(d)$;

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

Обработка результатов работы одного эксперта, в свою очередь, включает следующие шаги:

– формирование оценок показателей полноты, связности и непротиворечивости подразделов (только для базовых разделов документа);

– формирование оценок показателей полноты, связности и непротиворечивости разделов;

– формирование обобщенных оценок разделов документа;

– вычисление интегральной оценки документа экспертом $I_n(d)$, $1 \le n \le N$.

3.1. Определение интегральной оценки документа одним экспертом

Оценка документа начинается с экспертной оценки требований, регламентированных стандартами. Каждый эксперт e_n независимо определяет оценки вида a_{kn} ($1 \le k \le K$, $1 \le n \le N$).

При использовании комбинированной шкалы результаты выставления лингвистических оценок $a_{1n},...,a_{Kn}$ экспертом e_n представляются вектором $\mathbf{b} = (b_{1n},...,b_{Kn})$ количественных оценок. Наиболее простым подходом для получения обобщенных оценок показателей качества является использование взвешенных аддитивных сверток и методов интервальной оценки.

Вычисление обобщенных оценок показателей полноты, связности, непротиворечивости разделов и подразделов. Оценки показателей полноты, связности, непротиворечивости разделов и подразделов могут вычисляться в виде взвешенных аддитивных сверток множества количественных оценок соответствующих регламентированных требований.

Пусть S_{des}, R_{bas} – количество описательных и базовых разделов в документе d соответственно. Оценка O_n^{st} s-го описательного раздела по t-му показателю (O_n^{s1} – полнота, O_n^{s2} – связность, O_n^{s3} – непротиворечивость s-го раздела), соответствующая эксперту e_n, вычисляется по формуле

$$O_n^{st} = \sum_{k=1}^{k^{st}} p(w_k^{st}) \cdot b_{kn}^{st}, \ \sum_{k=1}^{k^{st}} p(w_k^{st}) = 1, \ 1 \le s \le S_{des}, \ 1 \le t \le 3, \qquad (1)$$

где $\{ w_1^{st}, \ldots, w_{k^{st}}^{st} \}$ – множество регламентированных требований, связанных с оценкой s-го раздела по t-му показателю; k^{st} – количество таких требований; $b_{1n}^{st}, \ldots, b_{k^{st}n}^{st}$ – количественные оценки уровня соответствия этим требованиям, которые сопоставлены лингвистическим оценкам, выставленным экспертом e_n; $p(w_1^{st}), \ldots, p(w_{k^{st}}^{st})$ – веса требований $w_1^{st}, \ldots, w_{k^{st}}^{st}$.

Соответствующую эксперту e_n обобщенную оценку t-го показателя (полноты, связности, непротиворечивости) q-го подраздела r-го базового раздела обозначим как O_n^{rqt} ($1 \le r \le R_{bas}$, $1 \le t \le 3$, $1 \le q \le k^r$). Вычисление количественных оценок подразделов базовых разделов может осуществляться по аналогии с (1).

Вычисление обобщенных оценок разделов ПЗ (ЗБ). Обобщенные оценки качества разделов могут вычисляться в виде взвешенных аддитивных сверток оценок показателей полноты, связности, непротиворечивости, полученных на предыдущем этапе. Обобщенная оценка O_n^s s-го описательного раздела, соответствующая эксперту e_n, $1 \le s \le S_{des}$, вычисляется по формуле

$$O_n^s = \sum_{t=1}^{3} p^{st} \cdot O_n^{st}, \ \sum_{t=1}^{3} p^{st} = 1,$$

где p^{st} – вес t-го показателя для s-го раздела. Обобщенная оценка O_n^r r-го базового раздела, соответствующая эксперту e_n, $1 \le r \le R_{bas}$, вычисляется по формуле

$$O_n^r = \sum_{q=1}^{k^r} p^{rq} \cdot \left(\sum_{t=1}^{3} p^{rqt} \cdot O_n^{rqt} \right), \ \sum_{t=1}^{3} p^{rqt} = 1 \ \text{для всех } 1 \le q \le k^r, \ \sum_{q=1}^{k^r} p^{rq} = 1,$$

где k^r – количество подразделов в r-м базовом разделе; p^{rqt} – вес t-го показателя для q-го подраздела r-го базового раздела; p^{rq} – вес подраздела в разделе.

Вычисление интегральной оценки качества ПЗ (ЗБ) одним экспертом. Вычислим интегральную оценку качества ПЗ (ЗБ) одним экспертом. Пусть p^r – вес r-го раздела, отражающий его значимость в оценке качества документа d. Количественная оценка $O_n(d)$ документа, соответствующая эксперту e_n, может вычисляться по формуле

$$O_n(d) = \sum_{r=1}^{R} p^r \cdot O_n^r, \ \sum_{r=1}^{R} p^r = 1,$$

где R – количество разделов в документе ($R = S_{des} + R_{bas}$). Заключение $I_n(d)$ эксперта e_n о качестве документа d формируется на основе оценки $O_n(d)$. Для отображения количественной оценки $O_n(d)$ в лингвистическую переменную $I_n(d) \in \{O_1, O_2, O_3, O_4, O_5\}$ можно использовать методы интервальной оценки [6]. При условии, что e_n проверил все регламентированные требования, решающее правило для формирования заключения будет следующим:

– если $O_n(d) \geq \delta_1$, то $I_n(d) = O_1$ («строгое соответствие»);

– если $\delta_2 \leq O_n(d) < \delta_1$, то $I_n(d) = O_2$ («высокий уровень соответствия»);

– если $\delta_3 \leq O_n(d) < \delta_2$, то $I_n(d) = O_3$ («средний уровень соответствия»);

– если $\delta_4 \leq O_n(d) < \delta_3$, то $I_n(d) = O_4$ («низкий уровень соответствия»);

– если $O_n(d) < \delta_4$, то $I_n(d) = O_5$ («несоответствие»).

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

Указанные пороговые значения определяются исходя из специфики конкретного объекта оценки и на основе анализа существующих для него рисков безопасности. Следует заметить, что методы анализа рисков составляют отдельную задачу и в данной статье не рассматриваются.

Таким образом, результирующее заключение о пригодности документа представляется в виде оценки его качества по лингвистической шкале O. При этом осуществляется обратный переход от количественной интегральной оценки документа к качественной. Соответствующая таблица перевода должна быть получена эмпирически после апробации предлагаемой методики оценки.

3.2. Определение общей интегральной оценки документа коллективом экспертов

Процедура определения общего коллективного заключения о качестве документа разбивается на два основных этапа: проверка отсутствия неприемлемо больших разногласий в мнениях экспертов, определение общей интегральной оценки $I(d) \in O$.

Проверка степени согласованности мнений экспертов. Проверка необходимой согласованности мнений экспертов может основываться на оценке отличия мнения каждого отдельного эксперта e_n от мнения коллектива экспертов в целом. Можно использовать, например, следующее правило оценки.

Пусть $\overline{O_k}$ – средняя количественная оценка требования w_k коллективом экспертов $e_1,\ldots,e_N$: $\overline{O_k}(d) = \frac{1}{N}\sum_{n=1}^{N} b_{kn}$. Мера σ_n отклонения оценок эксперта e_n может вычисляться по формулам

$$\sigma_n = \frac{1}{K}\sum_{k=1}^{K} p'(w_k)\cdot(b_{kn} - \overline{O_k}),$$

$$p'(w_k) = \begin{cases} p^r\, p(w_k), & \text{если } w_k \text{ – требование из } r\text{-го описательного раздела;} \\ p^r\, p^{rq}\, p(w_k), & \text{если } w_k \text{ – требование из } q\text{-го подраздела } r\text{-го базового раздела,} \end{cases}$$

где p^r, $1 \leq r \leq R$, – вес r-го раздела; p^{rq}, $1 \leq q \leq k^r$, – вес q-го подраздела r-го раздела.

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

$$\sigma_n \leq \delta^*, \ \forall\, n,\ 1 \leq n \leq N. \qquad (2)$$

Если для эксперта e_n, $1 \leq n \leq N$, выполняется условие $\sigma_n > \delta^*$, то принимается решение о неприемлемо большом отклонении в его оценке документа от оценок остальных экспертов. По отношению к каждому из этих экспертов могут быть выбраны, например, такие стратегии:

– предложить дать обоснование своих результатов оценки;

– провести совместное обсуждение результатов оценки эксперта и принять одно из 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 документа. Общая интегральная оценка $I(d) \in O$ определяется после обеспечения выполнения условия (2). Выбор общего заключения $I(d)$ 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 $\delta_{I(d)}$. Пороговое значение определяется с участием заказчика.

В случае отсутствия заключения, удовлетворяющего подобному условию, требуется скорректировать выбранные значения δ^*, $\delta_{I(d)}$ и повторить всю процедуру заново.

В целом в рамках предлагаемого подхода экспертам требуется задать 15 «настраиваемых» пороговых значений – δ_1, δ_2, δ_3, δ_4, δ^*, $\delta_{I(d)}$ и пороговые значения, определяющие интервалы количественных оценок соответствия лингвистических и количественных оценок (см. табл. 1 и 2). Отметим, однако, что при оценке каждого нового ПЗ (ЗБ) эксперты могут опираться на уже накопленный опыт и использовать сведения о пороговых значениях, показавших свою правомерность при проведении предыдущих оценок. Как показывает практика, чаще всего можно использовать уже применявшиеся ранее пороговые значения (возможно, предварительно произведя их незначительную корректировку).

3.3. Возможные направления совершенствования метода

В настоящей статье излагается наиболее простой подход к реализации предлагаемой методики оценки. Впоследствии предполагается его дальнейшее усовершенствование, в частности, в отношении методов обработки экспертных данных. Использование таких простых методов, как аддитивные свертки и интервальные методы, может не позволить в достаточной степени учесть специфику экспертных данных и тем самым негативно повлиять на достоверность оценок. Одним из хорошо зарекомендовавших себя на практике является подход, который основывается на использовании моделирования по прецедентности, реализуемого в рамках теории распознавания образов [7]. Такой подход позволяет учесть многие скрытые плохо формализуемые закономерности и эффективно использовать накопленный опыт.

Построение обучающей выборки. Обучающая информация содержит сведения об опыте, накопленном в процессе оценки документа для разных типовых объектов. Пусть $D = \{d_l \mid 1 \le l \le L\}$ – представительная выборка документов, которые уже прошли успешную оценку (L – достаточно велико). Обучающая информация состоит из множества Z векторов усредненных экспертных количественных оценок регламентированных требований по каждому ПЗ(ЗБ) и множества I вынесенных на их основании заключений о качестве ПЗ(ЗБ): $Z = \{\mathbf{z}_1 = (b_1(d_1), b_2(d_1), \dots, b_K(d_1)), \dots, \mathbf{z}_L = (b_1(d_L), b_2(d_L), \dots, b_K(d_L))\}$, $I = (I_1, \dots, I_L)$, где $I_j \in O$, $1 \le j \le L$, – заключение о качестве документа d_j.

Множество Z представляется в виде разбиения на пять классов

$$Z = \bigcup_{i=1}^{5} Z_i , \qquad (3)$$

где $Z_1 = \{\mathbf{z}_j \in Z \mid I_j = \text{«строгое соответствие»}\}$; $Z_2 = \{\mathbf{z}_j \in Z \mid I_j = \text{«высокий уровень соответствия»}\}$; $Z_3 = \{\mathbf{z}_j \in Z \mid I_j = \text{«средний уровень соответствия»}\}$; $Z_4 = \{\mathbf{z}_j \in Z \mid I_j = \text{«низкий уровень соответствия»}\}$; $Z_5 = \{\mathbf{z}_j \in Z \mid I_j = \text{«несоответствие»}\}$.

Принятие решения на основе распознавания по прецедентности. Пусть d – новый подлежащий оценке документ. В предположении репрезентативности обучающей выборки формирование заключения $I(d)$ может быть сведено:

– к оценке экспертом регламентированных требований и определению соответствующего вектора количественных оценок $\mathbf{b} = (b_1(d), b_2(d), \ldots, b_K(d))$;

– классификации вектора **b** относительно разбиения (3);

– выбору заключения, соответствующего классу, к которому был отнесен вектор **b**.

В качестве критерия разбиения можно использовать, например, критерий разбиения типа ближайшего соседа (в частности, отнесение **b** к классу, которому принадлежит ближайший к нему (относительно заданной функции близости) элемент из Z.

С учетом изложенной выше многоуровневой природы процесса оценки можно предложить, например, следующую функцию близости f. Пусть $(a_1,\ldots,a_K)$, $(b_1,\ldots,b_K) \in Z$. Используя введенные выше обозначения, получим

$$f(a,b) = \sqrt{\sum_{r=1}^{R_{bas}} p^r \cdot \sum_{q=1}^{k^r} p^{rq} \cdot \sum_{k=1}^{k^{rq}} p(w_k^{rq}) \cdot (a_k^{rq} - b_k^{rq})^2 + \sum_{s=1}^{S_{des}} p^s \cdot \sum_{k=1}^{k^s} p(w_k^s) \cdot (a_k^s - b_k^s)^2} \,, \qquad (4)$$

где k^r – количество подразделов в r-м базовом разделе; k^{rq} – количество регламентированных требований в q-м подразделе базового r-го раздела; k^s – количество регламентированных требований в s-м описательном разделе документа d.

4. Практическая реализация предлагаемого подхода

Рассмотрим общую характеристику разрабатываемого программного комплекса автоматизированной оценки качества ПЗ (ЗБ), реализующего предлагаемый подход [8]. База знаний программного комплекса включает экранные страницы экспертной оценки каждого требования, регламентированного стандартом, страницы с комментариями и примерами проведения оценки по предлагаемой методике, справочную информацию и др.

Процесс оценки ПЗ (ЗБ) экспертом представляется последовательностью выполнения девяти этапов (рис. 3). Оценка начинается с ввода в базу данных системы идентификационных данных эксперта и ПЗ (ЗБ). После этого производится настройка интервальной шкалы для формирования системы весовых коэффициентов, а также шкалы для ввода экспертных оценок выполнения требований. Пороговые значения отдельных интервалов могут изменяться. На этом подготовительный этап оценки заканчивается. Затем эксперт анализирует каждое требование безопасности и комментарии к нему и на этой основе устанавливает вес требования и оценку качества его реализации в документе. После анализа всех требований, характеризующих данный показатель, устанавливается его вес. Последовательно анализируя требования и показатели рассматриваемого раздела, эксперт устанавливает вес раздела.

На завершающем этапе, т. е. после анализа всех разделов, выполняется автоматизированное вычисление обобщенных оценок показателей качества подразделов, разделов и интегральной оценки документа в целом в числовой форме. Интегральные оценки показателей качества документа получаются на основе оценок экспертом степени выполнения всех регламентированных требований.

Результаты оценки сохраняются в БД «Эксперты» для каждого из документов, оцененных данным экспертом. В следующем сеансе работы с системой эксперт может вернуться к оценке любого из документов, над которыми он работал ранее. При этом диалоговые окна экспертной оценки отдельных требований инициализируются данными из БД «Эксперты». Полученная интегральная оценка преобразуется в лингвистическую по принятой шкале перевода. Принимается решение относительно итоговой оценки ПЗ (ЗБ). После работы всех экспертов определяется общая коллективная количественная оценка качества документа с ее переводом в качественную. По итогам оценки формируется экспертное заключение, составляется протокол оценки и технический отчет. Результаты оценки помещаются в БД системы. Накопленные в БД знания могут быть использованы при оценке новых документов.

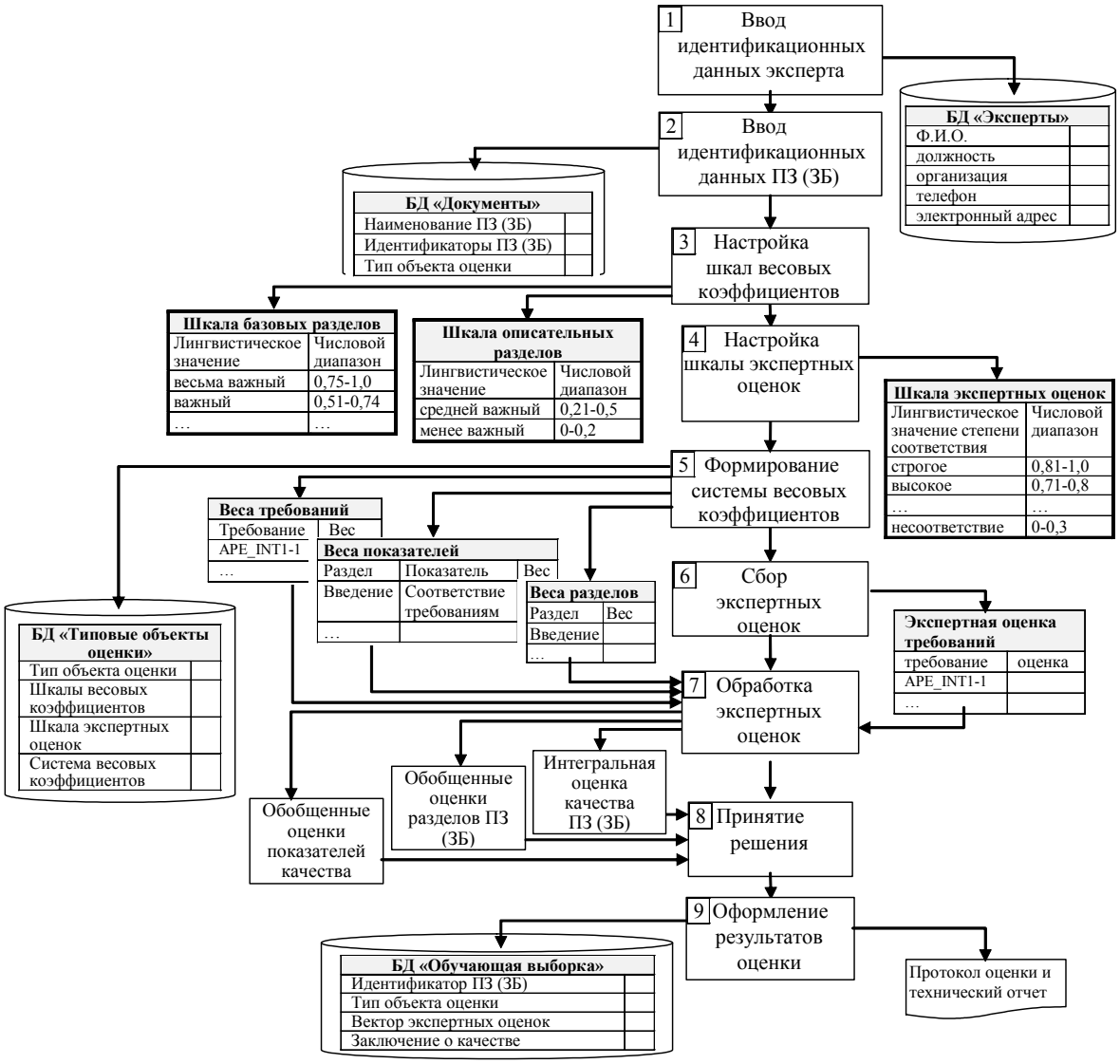

Рис. 3. Организационно-функциональная схема процедуры проведения экспертом оценки ПЗ (ЗБ)

Программный комплекс автоматизированной оценки качества ПЗ (ЗБ) включает следующие программные средства: ведения БД «Документы» и «Эксперты»; настройки процесса оценки (блоки 3, 4); ввода весовых коэффициентов, характеризующих важность разделов, показателей и отдельных требований (блок 5); ввода экспертных оценок качества документа (блок 6); обработки результатов экспертной оценки документов (блок 7) и информационной поддержки процесса принятия решения по выставлению интегральной оценки (блок 8); формирования протокола оценки в виде текстового файла (блок 9).

Заключение

Предложенная методика оценки качества ПЗ (ЗБ) и основанная на ней автоматизированная система поддержки принятия решения позволят: гарантировать соответствие процесса оценки действующим стандартам; значительно снизить трудоемкость процесса оценки; повысить обоснованность результата оценки; накапливать и эффективно использовать опыт тестирования разных типов объектов информационных технологий.

Изложенный подход предполагается реализовать в рамках программ фундаментальных исследований или программ защиты информации в виде соответствующего инструментально-

программного средства, которое, как представляется, будет полезно для испытательных лабораторий, занимающихся оценкой объектов информационных технологий.

Список литературы

1. Информационные технологии и безопасность. Профиль защиты. Разработка, обоснование, оценка : СТБ П 34.101.7–2003. – Минск : Госстандарт : Белорус. гос. ин-т стандартизации и сертификации, 2003. – 43 с.

2. Информационные технологии и безопасность. Задание по обеспечению безопасности. Разработка, обоснование, оценка : СТБ П 34.101.6–2003. – Минск : Госстандарт : Белорус. гос. ин-т стандартизации и сертификации, 2003. – 51 с.

3. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3 : Гарантийные требования безопасности : СТБ 34.101.3–2004. – Минск : Госстандарт : Белорус. гос. ин-т стандартизации и сертификации, 2003. – 112 с.

4. Information technology and security Evaluation criteria for Information technology security. Part 3: Security assurance requirements : ISO/MEC 15408–3–1999.

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. Краснопрошин, В.В. Проблема принятия решений по прецедентности, разрешимость и выбор алгоритмов / В.В. Краснопрошин, В.А. Образцов // Выбр. навук. працы Беларус. дзярж. ун-та. – 2001. – Т. 6. Матэматыка. – С. 285–312.

8. Максимович, Е.П. Методика и программные средства анализа и оценки качества профилей защиты и заданий по безопасности / Е.П. Максимович, В.К. Фисенко, М.С. Шибут // Технические средства защиты информации : материалы VII Белорус.-рос. науч.-техн. конф., Нарочь, Беларусь, 19–22 мая 2008 г. / Белорус. гос. ун-т информатики и радиоэлектроники. – Минск : БГУИР, 2008. – С. 92.

Поступила 21.03.08

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: m_shi@tut.by

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

AN APPROACH FOR AUTOMATION OF QUALITY ESTIMATION OF PROTECTION STRUCTURES AND SECURITY TASKS

An approach for automation of the processes of quality estimation of protection structures and the security tasks is suggested. It is in agreement with the Common criteria requirements and is based on definition of hierarchical system of quality parameters and fuzzy formalization. Implementation of the approach will essentially reduce laboriousness of the estimation process and will increase validity of decisions.