Література

1. Бакаев А. А. Международные транспортные коридоры Украины: сети и моделирование / А. А. Бакаев, С. И. Пирожков и др. – К., 2003. – 518 с.

2. Блудова Т. В. Транзитний потенціал України: формування та розвиток / Блудова Т. В. – К. : НІПМБ, 2006. – 274 с.

3. Денисенко С. І. Рамкові стандарти у міжнародних торговельних операціях / С. І. Денисенко // Зовнішня торгівля: право та економіка. – 2008. – № 4 (39). – С. 64–69.

4. Павленко Б. Є. Концептуальні підходи до впровадження Рамкових стандартів безпеки SAFE та їх роль у процесах боротьби з контрабандою [Електронний ресурс] / Б. Є. Павленко. – Режим доступу : http://www.nbuv.gov.ua.

5. Концепція розвитку транспортно-дорожнього комплексу України на середньостроковий період та до 2020 року / Міністерство транспорту України. – К., 2001.

6. Про транзит вантажів : Закон України від 20.09.1999 р. № 1172-XIV із змінами і доповненнями.

7. Рамкові стандарти ВМО [Електронний ресурс]. – Режим доступу : http://ambu.org.ua/files/ram_standart.html.

8. Правдин Н. В. Взаимодействие различных видов транспорта / Правдин Н. В., Негрей В. Я., Подкопаев В. А.; под ред Н. В. Правдина. – М. : Транспорт,1989. – 208 с.

9. Customs in the 21st Century. World Customs Organization [Електронний ресурс]. – Режим доступу : www.wcoomd.org.

10. Державний комітет статистики України [Електронний ресурс]. – Режим доступу : http://www.ukrstat.gov.ua.

✧ ✧ ✧ ✧ ✧ ✧ ✧

УДК 629.735

А. В. Потий, доктор технических наук,
начальник кафедры радиоэлектронных систем
управления воздушных сил
Харьковского университета
Воздушных сил им. И. Кожедуба
Д. С. Комин, адъюнкт Харьковского университета
Воздушных сил им. И. Кожедуба

ФОРМАЛЬНОЕ ОПИСАНИЕ ПРОЦЕССА ОЦЕНИВАНИЯ ГАРАНТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Наведено результати формального опису процесу оцінювання гарантій інформаційної безпеки. Вводяться визначення і формальні умови виконання вимог, які висуваються до результатів оцінювання (повторюваність, відтворюваність, зіставність).

Представлены результаты формального описания процесса оценивания гарантий информационной безопасности. Вводятся определения и формальные условия выполнения требований, которые предъявляются к результатам оценивания гарантий (повторяемость, воспроизводимость, сопоставимость).

Results of assurance evaluation formal specification are given. Definitions and formal conditions of repeatability, reproducibility and comparability requirements are introduce.

Ключевые слова. Требования гарантий, оценивание, экспертиза, процессный подход.

Введение. Важной составляющей оценки защищенности информационно-коммуникационных систем является экспертная оценка уровня гарантий защищенности. Такая оценка проводится в соответствии с требованиями международного стандарта ISO/IEC 15408 [1, 2] и национального нормативного документа НД ТЗИ 2.5-004-99 [3].

Результаты онтологического моделирования [4, 5] предметной области оценивания гарантий безопасности, требования к которым излагаются в национальных и международных нормативных документах [1, 2, 3, 6, 7, 8], других работах [9], показали, что к процессу оценивания предъявляются требования ширины, глубины и строгости, а к результатам оценивания – требования объективности, беспристрастности, повторяемости, воспроизводимости и сопоставимости [4, 5].

В [10] указывается, что достоверность и полнота результатов экспертизы достигается реализацией таких принципов:

– независимость организаторов экспертизы и экспертов;

– полнота оценивания;

– оценивание на основании полученных свидетельств;

– достоверность свидетельств оценивания;

– компетентность экспертов;

– этичность поведения экспертов.

В свою очередь, эксперты должны придерживаться таких основных принципов оценивания: объективность, беспристрастность, повторяемость, воспроизводимость, корректность, достаточность, приемлемость. Выдвижение таких требований вполне естественно, поскольку заказчик экспертизы должен получить определенные заверения в качестве организации и проведения экспертизы и валидности ее результатов.

Обзор доступной нормативной и научной литературы показал, что на сегодняшний день пути (способы, методы) достижения и обеспечения указанных требований не определены. Это обусловлено:

– недостаточной глубиной изучения самой природы данных требований;

– отсутствием формальной формулировки и представления требований (требования описаны лишь в качественной (вербальной) форме);

– отсутствием формальной постановки задачи на обеспечение данных требований;

– отсутствием формальных моделей процесса проведения экспертизы (оценивания) и формального представления результатов.

Постановка задачи. В данной работе решается задача формального описания процесса экспертной оценки гарантий безопасности с позиций процессного подхода и формального представления требований, которые предъявляются к результатам экспертизы.

Результаты исследования.

1. Формальная модель процесса оценивания гарантий

К оцениванию гарантий информационной безопасности предлагается подходить с позиций процессного подхода [11], то есть оценивание рассматривать как процесс. В работах [11–13] рассматриваются общие признаки любого процесса, а также анализируются различные определения процесса. Опираясь на эти результаты, дадим следующее определение.

Определение 1. Процесс оценивания требований гарантий информационной безопасности – это совокупность взаимосвязанных операций и действий, направленных на исследование, проверку, анализ и оценку объекта экспертизы, путем преобразования входных материальных и информационных потоков в выходные потоки, представляющие интерес для субъектов экспертизы, с целью определения (установления) степени соответствия характеристик объекта экспертизы заданным требованиям и определения возможности использования оцениваемого объекта в качестве доверенного с точки зрения безопасности информации.

В основу формальной модели процесса оценивания требований гарантий информационной безопасности положим следующие аксиоматические конструкции.

А1. Процесс оценивания требований гарантий составляет набор (множество) действий $A = \{A_n | n = \overline{1, N}\}$ по оцениванию гарантий.

Действия описывают работы, которые выполняют эксперты и другие участники процесса оценивания. В общем случае совокупность действий может быть представлена в виде графа G^A, который описывает конкретные типы отношений на множестве действий. Множество действий составляет методику оценивания.

А2. Множество отношений $D = \{D_m | d = \overline{1, M}\}$ различного типа, определенных на множестве A.

Множество действий A образует процесс $Z(A, d)$, если $A \in \overline{A}$, и на этом множестве задано отношение $d(A) \in D$. Отношение d может быть, например, отношением типа "часть – целое", "казуальная зависимость", "экзистенциональная зависимость" и др. Универсальное множество действий по оценке гарантий $\overline{A}$ определяется в нормативных документах [6, 7]. Для образования процесса на множестве A необходимо как минимум задать отношения зависимости (доминирования). В этом случае множество действий может рассматриваться как последовательность действий.

А3. Назначение процесса формируется целью *TRG* и ожидаемыми результатами *REZ*

$$Purpose = < TRG, REZ >. \quad (1)$$

Процесс реализуется и выполняется для достижения конкретной и ясной цели и получения результатов, представляющих интерес для участников процесса. Цель выступает системообразующим фактором и определяет отношения на множестве действий. В контексте оценивания гарантий безопасности главной целью выступает установление степени удовлетворения заданного множества требований гарантий и соответствия объекта экспертизы определенному уровню гарантий безопасности.

Главная цель может быть декомпозирована на подцели, в частности на совокупность свойств $P = \{P_j | j = \overline{1, J}\}$, которыми должен обладать объект экспертизы для удовлетворения требований гарантий. Множество свойств может быть представлено в виде графа $G^P = \{P, D\}$, где D – множество отношений, устанавливаемых на множестве свойств. Множество свойств составляет программу оценивания *Pr*.

В качестве результата *REZ* процесса оценивания выступает множество заключений (вердиктов) экспертов $V = \{V_i | i = \overline{1, I}\}$ относительно степени проявления отдельных свойств гарантий безопасности. Эти вердикты оформляются в виде отчета, что является материальным выражением результата оценивания гарантий безопасности. Анализ требований гарантий, закрепленных нормативными документами [2, 3], позволил сделать вывод, что требования в большей степени носят качественный характер, и количественно выражены быть не могут. Это усложняет их анализ и формальное представление. Одним из путей решения данной задачи является использование аппарата лингвистических переменных, позволяющего задавать формальные значения переменных в виде вербальных выражений. При использовании такого подхода [14, 15] для каждого свойства вводится лингвистическая переменная L и определяется ее терм-множество β_L, то есть множество значений, которые она может принимать. Следовательно, каждый вердикт является отражением значения лингвистической переменной, которое она приняла в ходе экспертизы. Формально можно сказать, что каждый вердикт V_i содержит значение лингвистической переменной i-го свойства, а сам отчет можно представить в виде множества значений лингвистических переменных $V = \{L_i | i = \overline{1, I}\}$.

Таким образом, назначение процесса оценивания гарантий безопасности будет формировать дерево целей G^P (которое описывается в программе оценивания) и множество вердиктов V, представленных в виде отчета:

$$Purpose = < G^P, V >. \quad (2)$$

А4. Множество входов $IN = \{I^{in}, M^{in}\}$ и выходов $OUT = \{I^{out}, M^{out}\}$ процесса Z с заданным оператором преобразования $F : IN \rightarrow OUT$.

В общем случае входы и выходы процесса представляют собой материальные и информационные потоки. Материальный поток M представляет собой непрерывное или дискретное множество материальных объектов $M = \{m_q | q = \overline{1, Q}\}$, распределенных во времени. Информационный поток I – это непрерывное или дискретное множество информационных объектов $I = \{i_n | n = \overline{1, N}\}$.

Процесс оценивания гарантий будет включать два потока: материальный – объект экспертизы *TOE* и материально-информационный – совокупность (множество) свидетельств E.

В отечественной нормативной документации [6, 10] в качестве объекта экспертизы на соответствие требованиям гарантий выступает средство технической защиты информации от несанкционированного доступа, под которым понимается программное, аппаратное или программно-аппаратное средство, которое создается как отдельный продукт производства, имеет необходимую проектную и/или эксплуатационную документацию и обеспечивает самостоятельно или в комплексе с другими средствами защиту от угроз несанкционированного доступа для информации, которая обрабатывается в информационно-телекоммуникационной системе. В международном стандарте [1] объект оценивания определен как совокупность программных, программно-аппаратных и аппаратных средств, которые могут сопровождаться руководствами.

В общем случае объект экспертизы (объект оценивания) *TOE* можно представить в виде:

$$TOE = <Hw, Sw, D>, \quad (3)$$

где $Hw = \{Hw_i | i = \overline{1, I}\}$ – аппаратные составляющие ОО; $Sw = \{Sw_j | j = \overline{1, J}\}$ – программные составляющие ОО; $D = \{D_z | z = \overline{1, Z}\}$ – комплект документации к ОО.

Оценивание ОО проводится на основании полученных свидетельств E. Основными источниками свидетельств являются полученные от заказчика экспертизы (разработчика объекта экспертизы) документы и материалы, устные высказывания и письменные ответы сотрудников организации заказчика экспертизы (разработчика объекта экспертизы), результаты наблюдений за этими сотрудниками, непосредственно объект экспертизы и его составные части. Полученная совокупность свидетельств формально может быть выражена в виде множества $E = \{e_y | y = \overline{1, Y}\}$, а при наличии связей наследования (иерархических зависимостей) – в виде графа G^E (или таблицы).

А5. Множество участников-субъектов процесса. В общем случае это

$$PS = (Own, Man, Per, Sup, Cus), \quad (4)$$

где *Own* – владелец процесса; *Man* – управляющий процессом; *Per* – исполнитель процесса; *Sup* – поставщик процесса; *Cus* – потребитель процесса. Множество участников процесса образуют команду *Process_team*, если на множестве *PS* определены роли *role* и полномочия

authority субъектов процесса, которые характеризуют отношения между участниками процесса, то есть

$$Process\_team\ (PS, role, authority). \quad (5)$$

В [1] субъектами экспертизы определены: юридические и физические лица, которые являются заказчиками экспертизы; уполномоченный государственный орган; подразделения уполномоченного государственного органа, предприятия, учреждения и организации, которые проводят экспертизу (организаторы экспертизы); государственные органы, которые проводят экспертизу в сфере своего управления; физические лица – исполнители экспертных работ (эксперты). В данном случае субъекты могут быть представлены в виде множества *PS*. В [16] автор глубоко проанализировал международный стандарт ISO/IEC 15408 [1, 2] и выявил субъекты, принимающие участие в процессе оценивания. Результаты такого анализа, ввиду наличия иерархических зависимостей между субъектами, могут быть представлены в виде графа G^{PS}.

Среди множества субъектов экспертизы (оценивания) нас будут интересовать эксперты *B*, то есть лица, выполняющие действия и принимающие решения относительно оценивания свойств гарантий (вынесения вердиктов). Подбор экспертов возлагается на организаторов экспертизы. Одним из методов подбора экспертов является выбор по формальным признакам, таким как: должность, образование, научная степень и учёное звание, стаж, компетентность, успешность участия в предыдущих экспертизах и др. Данные признаки могут быть использованы при сравнении экспертов. Для этого их необходимо представить в виде множества $B_i = \{b_{ix} | x = \overline{1, X}\}$, где X – количество формальных признаков, i – i-й эксперт.

А6. Множество финансовых *F*, временных *T*, трудовых *L*, экономических *E*, материальных *Mat* и иных ресурсов, необходимых для реализации и выполнения процесса *Z:*

$$Resource = \{F, T, L, E, Mat\}. \quad (6)$$

Опираясь на введенные конструкции А1–А6, можно представить следующую формальную модель процесса оценивания гарантий:

$$Z = < Pur\ (G^P, V),\ d(A),\ F(TOE, E) : IN \rightarrow OUT,\ Process\_team\ (B),\ Resource >. \quad (7)$$

Данная модель может рассматриваться как базовая и использоваться для дальнейших исследований процесса оценивания гарантий информационной безопасности.

2. Формальное описание требований, предъявляемых к результатам оценивания гарантий

В контексте предложенной модели процесса оценивания гарантий информационной безопасности дадим формальные определения требованиям, предъявляемым к результатам экспертизы.

2.1. Объективность

Определение 2. Объективность – свойство, которое предполагает, что результаты оценки гарантий безопасности должны быть фактическими, то есть не подверженными влиянию чувств или мнений эксперта (оценщика).

Объективность может быть обеспечена при условии, что результаты оценивания получены путем исследования предоставленных свидетельств и у эксперта есть уверенность в достоверности этих свидетельств. Объективность результатов тесно пересекается с требованием беспристрастности результатов оценивания.

2.2. Беспристрастность

Определение 3. Беспристрастность – свойство, которое предполагает, что оценка гарантий безопасности не должна быть предубежденной по отношению к любому результату оценивания.

Беспристрастность обеспечивается независимостью организаторов экспертизы и экспертов, которые проводят оценивание. Эксперты не должны быть причастны к организации – заказчику экспертизы и к разработчикам (разработке) объекта, подлежащего экспертизе. То есть экспертами могут быть лишь те люди (организации), для которых может быть документально подтверждена их непричастность к любой из стадий разработки оцениваемого объекта, в том числе консультационных услуг, которые касаются выполнения определенных этапов работ по созданию объекта оценивания, обоснования и выбора определенных проектных решений.

Таким образом, беспристрастность обеспечивается процедурой организации экспертизы, закрепленной в нормативных актах.

2.3. Повторяемость

Определение 4. Повторяемость – свойство, которое обеспечивает идентичность результатов оценивания при повторной оценке одного и того же ОО, которая проводится по той же программе и методике оценки гарантий безопасности, тем же экспертом (оценщиком), с использованием одной и той же совокупности (множества) свидетельств.

В общем виде схема выполнения требования повторяемости будет иметь вид:

$Z_{(t_0, t_1)}$		$Z_{(t_2, t_3)}$	
(t_0, t_1)	$\neq$	(t_2, t_3)	– время проведения экспертизы
TOE_1	=	TOE_2	– объект оценивания
Pr_1	=	Pr_2	– программа оценивания
A_1	=	A_2	– методика оценивания
B_1	=	B_2	– эксперт
E_1	=	E_2	– совокупности свидетельств
V_1	=	V_2	– результаты оценивания

В контексте данного определения возникает задача сравнения отдельных элементов модели процесса оценивания гарантий. Для решения данной задачи введем формальные условия сравнения некоторых элементов модели.

Условие 1. Два ОО TOE_1 и TOE_2 идентичны, если выполняется условие равенства множеств соответствующих их составляющих:

$$\text{IF } (\{Hw_i | i = \overline{1, I}\}_{TOE_1} = \{Hw_i | i = \overline{1, I}\}_{TOE_2}, \{Sw_j | j = \overline{1, J}\}_{TOE_1} =$$

$$= \{Sw_j | j = \overline{1, J}\}_{TOE_2}, \{D_z | z = \overline{1, Z}\}_{TOE_1} = \{D_z | z = \overline{1, Z}\}_{TOE_2}) \text{ THEN } TOE_1 = TOE_2. \quad (8)$$

Если при сравнении двух ОО условие равенства хотя бы одной пары множеств не выполняется, то ОО являются неидентичными.

Условие 2. Две программы оценивания Pr_1 и Pr_2 идентичны (равны), если выполняется условие равенства графов $G^P_{\text{Pr}_1} = G^P_{\text{Pr}_2}$ и их матриц смежности $(p_{ij})_{\text{Pr}_1} = (p_{ij})_{\text{Pr}_2}$:

$$IF\ (G^{P}_{Pr_1} = G^{P}_{Pr_2},\ (p_{ij})_{Pr_1} = (p_{ij})_{Pr_2}, i = \overline{1,m},\ j = \overline{1,n})\ THEN\ Pr_1 = Pr_2. \quad (9)$$

Если условие равенства не выполняется, то программы различны.

Условие 3. Две методики A_1 и A_2 идентичны, если выполняется условие равенства графов $G^{A}_{A_1} = G^{A}_{A_2}$ и их матриц смежности $(a_{ij})_{A_1} = (a_{ij})_{A_2}$.

$$IF\ (G^{A}_{A_1} = G^{A}_{A_2}\ \text{и}\ (a_{ij})_{A_1} = (a_{ij})_{A_2}, i = \overline{1,m},\ j = \overline{1,n})\ \text{THEN}\ A_1 = A_2. \quad (10)$$

Если условие равенства не выполняется, то методики различны.

Условие 4. Два эксперта B_1 и B_2 идентичны, если выполняется условие равенства множеств их формальных признаков

$$IF\ (B_{1x}|x = \overline{1,X}\ \} = \{B_{2x}|x = \overline{1,X}\ \})\ \text{THEN}\ B_1 = B_2. \quad (11)$$

Если условие равенства множеств не выполняется, то эксперты различны.

Условие 5. Две совокупности свидетельств E_1 и E_2 идентичны (равны), если выполняется условие равенства множеств

$$IF\ (\{e_y|y = \overline{1,Y}\}_{E_1} = \{e_y|y = \overline{1,Y}\}_{E_2})\ \text{THEN}\ E_1 = E_2, \quad (12)$$

либо равенство графов и матриц их смежности

$$IF\ (G^{E}_{E_1} = G^{E}_{E_2}\ \text{и}\ (e_{ij})_{E_1} = (e_{ij})_{E_2}, i = \overline{1,m},\ j = \overline{1,n})\ \text{THEN}\ E_1 = E_2. \quad (13)$$

Если условие равенства не выполняется, то совокупности свидетельств различны.

Условие 6. Два отчета V_1 и V_2 идентичны (равны), если выполняется условие равенства множеств значений лингвистических переменных соответствующих отчетов $\{L_i|i = \overline{1,I}\}_{V_1}$ и $\{L_i|i = \overline{1,I}\}_{V_2}$:

$$IF\ (\{L_i|i = \overline{1,I}\}_{V_1} = \{L_i|i = \overline{1,I}\}_{V_2})\ \text{THEN}\ V_1 = V_2. \quad (14)$$

Если условие равенства не выполняется, то отчеты по оцениванию различны.

Опираясь на условия 1–6 и определение 4, введем формальное условие повторяемости.

Условие 7. Результаты оценивания гарантий считаются *повторяемыми*, если объект оценивания *TOE* был подвержен двум экспертизам (15) и (16):

$$Z_{(t_0,t_1)} = < Pur\ (Pr_1, V_1),\ d(A_1),\ F(TOE_1, E_1) : IN \rightarrow OUT,\ Process\_team\ (B_1),\ Resource > \quad (15)$$

$$Z_{(t_2,t_3)} = < Pur\ (Pr_2, V_2),\ d(A_2),\ F(TOE_2, E_2) : IN \rightarrow OUT,\ Process\_team\ (B_2),\ Resource > \quad (16)$$

в промежутки времени (t_0, t_1) и (t_2, t_3) соответственно, выполняются условия: идентичности объектов оценивания $TOE_1 = TOE_2$ (8), идентичности программ оценивания $Pr_1 = Pr_2$ (9), идентичности методик оценивания $A_1 = A_2$ (10), идентичности экспертов $B_1 = B_2$ (11), идентичности совокупности свидетельств $E_1 = E_2$ (12 или 13), и при этом обеспечивается условие идентичности результатов экспертизы $V_1 = V_2$ (14).

Таким образом, условие повторяемости говорит о том, что результаты экспертизы являются инвариантными по времени.

2.4. Воспроизводимость

Определение 5. Воспроизводимость – свойство, которое обеспечивает идентичность результатов оценивания при повторной оценке одного и того же ОО, которая проводится по той же программе и методике оценке гарантий безопасности различными экспертами (оценщиками), с использованием одной и той же совокупности (множества) свидетельств.

В общем виде схема выполнения требования воспроизводимости будет иметь вид:

$Z_{(t_0, t_1)}$		$Z_{(t_2, t_3)}$	– номер экспертизы
(t_0, t_1)	$\neq$	(t_2, t_3)	– время проведения экспертизы
TOE_1	=	TOE_2	– объект оценивания
Pr_1	=	Pr_2	– программа оценивания
A_1	=	A_2	– методика оценивания
B_1	$\neq$	B_2	– эксперт
E_1	=	E_2	– совокупности свидетельств
	⇩		
V_1	=	V_2	– результаты оценивания

Опираясь на условия 1–6 и определение 5, введем формальное условие воспроизводимости.

Условие 8. Результаты оценивания гарантий считаются *повторяемыми*, если объект оценивания *TOE* был подвержен двум экспертизам (17) и (18):

$$Z_{(t_0,t_1)} = < Pur\ (Pr_1, V_1),\ d(A_1), F(TOE_1, E_1) : IN \rightarrow OUT,\ Process\_team\ (B_1),\ Resource > \quad (17)$$

$$Z_{(t_2,t_3)} = < Pur\ (Pr_2, V_2),\ d(A_2), F(TOE_2, E_2) : IN \rightarrow OUT,\ Process\_team\ (B_2),\ Resource > \quad (18)$$

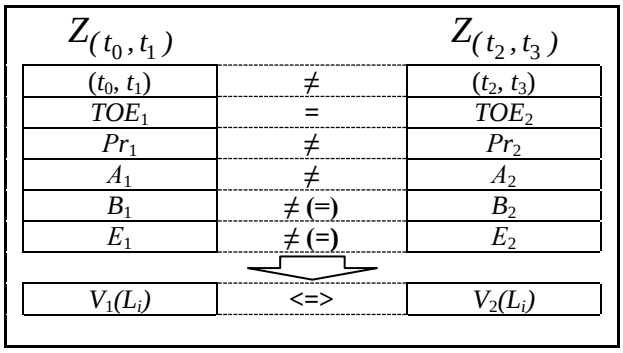
в промежутки времени (t_0, t_1) и (t_2, t_3) соответственно, выполняются условия: идентичности объектов оценивания $TOE_1 = TOE_2$ (8), идентичности программ оценивания $Pr_1 = Pr_2$ (9), идентичности методик оценивания $A_1 = A_2$ (10), неидентичности экспертов $B_1 \neq B_2$ (11), идентичности совокупности свидетельств $E_1 = E_2$ (12 или 13), и при этом обеспечивается условие идентичности результатов экспертизы $V_1 = V_2$ (14).

Таким образом, из условия воспроизводимости следует, что результаты экспертизы являются инвариантными по времени и экспертам.

2.5. Сопоставимость

Определение 6. Сопоставимость – свойство, которое обеспечивает сравнимость результатов оценивания, полученных при оценке одного и того же ОО по различным программам и методикам оценивания различными (или одним и тем же) экспертами.

В общем виде схема выполнения требования сопоставимости будет иметь вид:



– номер экспертизы
– время проведения экспертизы
– объект оценивания
– программа оценивания
– методика оценивания
– эксперт
– совокупности свидетельств
– результаты оценивания

Опираясь на условия 1–6 и определение 6, введем формальное условие сопоставимости.

Условие 9. Результаты оценивания гарантий считаются *сопоставимыми*, если объект оценивания *TOE* был подвержен двум экспертизам (19) и (20):

$$Z_{(t_0,t_1)} = < Pur\ (Pr_1, V_1),\ d(A_1),\ F(TOE_1, E_1) : IN \rightarrow OUT,\ Process\_team\ (B_1),\ Resource > \quad (19)$$

$$Z_{(t_2,t_3)} = < Pur\ (Pr_2, V_2),\ d(A_2),\ F(TOE_2, E_2) : IN \rightarrow OUT,\ Process\_team\ (B_2),\ Resource >, \quad (20)$$

в промежутки времени (t_0, t_1) и (t_2, t_3) соответственно, выполняются условия: идентичности объектов оценивания $TOE_1 = TOE_2$ (8), неидентичности программ оценивания $Pr_1 \neq Pr_2$ (9), неидентичности методик оценивания $A_1 \neq A_2$ (10), идентичности либо неидентичности экспертов $B_1 = (\neq)\ B_2$ (11), идентичности либо неидентичности совокупности свидетельств $E_1 = (\neq)\ E_2$ (12 или 13), и при этом обеспечивается условие сравнимости результатов экспертизы $V_1(L_i) <=> V_2(L_i)$.

Условие сравнимости определяет сравнимость результатов, то есть наличие у сравниваемых результатов признаков или характеристик, дающих основание для сравнения. Так как отчеты представляются в различных формах, то такие признаки могут быть получены в ходе анализа результатов оценивания. Например, если при разработке программы оценивания *Pr* для каждого свойства P_i была введена лингвистическая переменная L_i, то в качестве критериев сравнения могут выступать соответствующие значения лингвистических переменных.

Выводы. В работе предложена формальная модель экспертизы и сформулированы условия идентичности объектов оценивания, программ оценивания, методик оценивания, экспертов, совокупности свидетельств и результатов оценивания.

В рамках введенных формальных условий в работе впервые предложены формальные определения условий повторяемости, воспроизводимости и сопоставимости результатов оценивания. Данные условия являются четкими и опираются на строгие определения равенства соответствующих множеств или графов, что позволяет на практике объективно подтвердить (доказать, обосновать) выполнение требований к результатам экспертизы.

Показано, что требования объективности и беспристрастности результатов оценивания обеспечиваются организацией экспертизы (институционными нормами), построением системы экспертизы в целом на государственном уровне.

Выявлено, что выполнение требований повторяемости и воспроизводимости результатов оценивания означает, что результаты оценивания должны быть инвариантными по времени и экспертам. Для обеспечения выполнения требования сопоставимости необходимо вводить условия (критерии) сравнения. Представление результатов оценивания гарантий в виде вербального описания усложняет введение таких критериев. Поэтому необходимо

дальнейшее изучение природы сравнимости и разработки способов сравнения вербальных результатов оценивания.

Литература

1/ ISO/IEC 15408-1:2009, Informational technology. – Security techniques. – Evaluation criteria for IT security. – Part 1 : Introduction and general model.

2. ISO/IEC 15408-3:2008, Informational technology. – Security techniques. – Evaluation criteria for IT security. – Part 3 : Security assurance requirement.

3. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28.04.1999 р. № 22.

4. Потий А. В. Системно-онтологический анализ предметной области оценивания гарантий информационной безопасности / А. В. Потий, Д. С. Комин // Радіоелектронні і комп'ютерні системи. – 2010. – № 5(46). – С. 50–56.

5. Потий А. В. Оценка гарантий информационной безопасности на основе функционально-лингвистического подхода / А. В. Потий, Д. С. Комин // Прикладная радиоэлектроника. – 2010. – Т. 9 (№ 3). – С. 421–435.

6. НД ТЗІ 2.7-010-09: Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу : затверджено наказом ДСТСЗІ СБ України від 24.07.2009 № 172.

7. ISO/IEC 18045:2005, Informational technology. – Security techniques. – Methodology for IT security evaluation.

8. ISO/IEC TR 15443:2005. Informational technology. – Security techniques. – A framework for IT security assurance. – Part 1 : Overview and framework.

9. Трубачев А. П. Оценка безопасности информационных технологий / А. П. Трубачев и др. – М. : СИП РИА, 2001. – 356 с.

10. НД ТЗІ 2.6-001-11: Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах : затверджено наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 25.03.2011 № 65.

11. Потий А. В. Формальная модель процесса защиты информации / А. В. Потий // Радіоелектронні і комп'ютерні системи. – 2006. – № 5 (17). – С. 128–133.

12. Потій О. В. Процесний підхід до управління безпекою інформації // Безопасность информации в ИТС : VIII международная научно-практическая конференция 11–13 мая 2005 : тезисы докладов. – К. : НИЦ Тезис, 2005. – С. 69–70.

13. Арчибальд Р. Управление высокотехнологичными программами и проектами / Арчибальд Р. – М. : Компания АйТи ; ДМК Пресс, 2004. – 472 с.

14. Потий А. В. Оценка гарантий безопасности на основе применения лингвистических переменных / А. В. Потий, Д. С. Комин // Системи обробки інформації. Інформаційна та економічна безпека. – 2010. – № 3 (84). – С. 34–37.

15. Потий А. В. Нечеткий логический вывод в задачах оценки уровня гарантий безопасности / А. В. Потий, Д. С. Комин // Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій : V міжнародна науково-практична конференція (Запоріжжя, 22–24 вересня 2010 р.). – З. : ЗНТУ, 2010. – С. 121–123.

16. Prieto-Diaz, R. The Common Criteria Evaluation Process. Process Explanation, Shortcomings, and Research Opportunities. – Commonwealth Information Security Center Technical Report CISC-TR-2002-03, December 2002. – CISC, James Madison University, USA. – 62 p.