УДК 681.03

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

МОДЕЛЬ ОЦЕНКИ КАЧЕСТВА ПРОФИЛЕЙ ЗАЩИТЫ И ЗАДАНИЙ ПО БЕЗОПАСНОСТИ С УЧЕТОМ ЭКСПЕРТНЫХ ЗНАНИЙ

Рассматривается задача формализации процесса использования накопленного опыта при разработке и оценке качества профилей защиты и заданий по безопасности. Полученные результаты могут быть использованы при создании автоматизированных систем поддержки принятия решений в области информационной безопасности.

Введение

Оценка качества профилей защиты (ПЗ) и заданий по безопасности (ЗБ) – важный этап оценки безопасности объектов информатизации (ОИ), обеспечивающий необходимый базис для проведения испытаний систем защиты информации ОИ. Методическими документами, используемыми в Республике Беларусь для оценки качества ПЗ и ЗБ, являются международные стандарты ISO/IEC 15408-3, ISO/IEC 18045 и национальный стандарт СТБ 34.101.3–2004 [1–3]. В соответствии с данными стандартами общий подход к оценке качества ПЗ (ЗБ) состоит в последовательном анализе экспертом разделов документа и проверке того, выполняются ли для них заданные совокупности регламентированных требований безопасности, на основании чего выносится заключение о качестве каждого отдельного раздела, а затем и документа в целом. Однако практическая реализация такого подхода связана с необходимостью решения целого ряда нетривиальных задач, к числу которых относится, например, уже рассмотренная ранее авторами проблема излишней категоричности используемых критериев принятия решений, для решения которой была предложена гибкая пятибалльная шкала оценки [4].

Настоящая статья посвящена еще одному важному вопросу – эффективному использованию накопленного опыта, полученного по результатам ранее проведенных оценок качества ПЗ (ЗБ). Задача эффективного использования накопленного опыта относится к числу важных проблем, часто возникающих при создании современных автоматизированных систем поддержки принятия решения в различных областях человеческой деятельности. Применительно к оценке качества ПЗ (ЗБ) актуальность этой задачи обусловлена следующим. Хотя стандарты и содержат общие рекомендации по проверке регламентированных требований к ПЗ (ЗБ), эффективность использования этих рекомендаций полностью зависит от квалификации эксперта и знания им специфичных слабых мест безопасности ОИ, для которого разработан оцениваемый документ. Это обусловливает важность разработки формализованных подходов, направленных на поддержку процесса оценки с целью уменьшения влияния субъективного фактора и трудозатрат, а также повышения обоснованности экспертных оценок. Ввиду плохой формализуемости процесса при разработке подобных подходов целесообразно базироваться на использовании уже накопленного опыта оценки.

В данной статье опыт трактуется как накопленные сведения, содержащиеся в следующих документах:

– ПЗ (ЗБ), уже прошедших успешную оценку и рассматриваемых как эталонные, с тем чтобы качество вновь разрабатываемых и предоставляемых на оценку ПЗ (ЗБ) было не ниже качества документов, ранее утвержденных органом оценки;

– протоколах оценки, содержащих информацию о типичных недостатках, обнаруженных ранее в уже оцененных ПЗ (ЗБ), с тем чтобы наиболее полно учесть возможные слабые места во вновь разработанных и предоставленных на оценку ПЗ (ЗБ).

Предлагаемый в статье подход позволяет совершенствовать процесс использования накопленного опыта за счет формирования:

– каталогов предположений, угроз, политик безопасности, задач безопасности и функциональных требований для ПЗ (ЗБ) различных типовых ОИ и последующего использования их

при разработке и оценке конкретных ПЗ (ЗБ). Каталоги создаются на основе ПЗ (ЗБ), ранее прошедших успешную оценку и утвержденных органом оценки. Использование каталогов способствует обеспечению общих показателей полноты, связности и непротиворечивости ПЗ (ЗБ) в ходе их разработки и оценки;

– каталогов возможных недостатков ПЗ (ЗБ) для различных типовых ОИ и последующего использования их при оценке конкретных ПЗ (ЗБ). Каталоги создаются на основе уже существующих протоколов экспертной оценки. Использование каталогов способствует обеспечению более тщательной оценки, а также позволяет вычислить некоторые рекомендуемые пороговые значения для выставляемых экспертом оценок [4].

1. Общие сведения

В рамках предлагаемого подхода к использованию накопленного опыта рассматриваются две основные задачи:

– формирование и сопровождение данных, составляющих опыт оценки ПЗ (ЗБ);

– использование опыта в процессе оценки ПЗ (ЗБ).

Первая задача включает формирование исходных данных, предварительную обработку и систематизацию исходных данных, текущую актуализацию и корректировку данных, составляющих опыт оценки.

Вторая задача включает использование положительного опыта разработки ПЗ (ЗБ), а также опыта о недостатках, допускаемых при разработке ПЗ (ЗБ).

2. Формирование исходных данных

ПЗ (ЗБ) содержат накопленный положительный опыт в части разработки данных документов. Протоколы оценки содержат накопленный отрицательный опыт в части возможных недостатков при разработке ПЗ (ЗБ), обнаруженных в ходе их экспертной оценки.

В протоколах оценки описываются результаты выполнения единиц работы, проведенных по проверке регламентированных стандартами требований. По каждой единице работы приводятся ее вес, выставленная экспертом оценка и описание выявленных недостатков. Вес единицы работы отражает ее важность с точки зрения оценки качества ПЗ (ЗБ). Оценка отражает степень выполнения соответствующего требования в оцениваемом ПЗ (ЗБ) и выставляется исходя из значимости обнаруженных (по данному требованию) недостатков.

В качестве шкал, используемых для формирования оценок и весов, используются комбинированные шкалы, предложенные в [4] и включающие перечень допустимых лингвистических оценок и соответствующие им числовые интервалы. Лингвистическая шкала оценки степени выполнения требований включает пять градаций: «строгое соответствие», «высокая степень соответствия», «средняя степень соответствия», «низкая степень соответствия», «несоответствие». Лингвистическая шкала важности требований включает четыре градации: «весьма важное», «важное», «средней важности», «наименее важное». Каждому лингвистическому значению сопоставляется числовой интервал значений количественных оценок, предназначенный для уточнения степени соответствия оцениваемого свойства документа выбранной лингвистической оценке.

В соответствии с [2] везде далее предполагается, что рассматриваются ПЗ (ЗБ), в которых заявлен не более чем четвертый уровень гарантии оценки (УГО).

3. Предварительная обработка и систематизация исходных данных

При использовании накопленного опыта оценки большое значение имеет предварительная фильтрация и систематизация составляющей его информации. Без этого в массе собранного материала практически невозможно будет найти необходимые полезные сведения и попытка использования опыта может не только не помочь, но и запутать эксперта. Особую актуальность придает вопросу предобработки тот факт, что на практике для накопления опыта используется, вообще говоря, множество источников сбора информации, вследствие чего накапливаемая информация обычно характеризуется противоречивостью, несогласованностью, дублированием,

фрагментарностью, зашумленностью (наличием несущественных сведений), возможным наличием непроверенных сведений.

Для предобработки данных используются методы интеллектуального анализа данных (добычи данных (Data Mining)), позволяющие структурировать и обобщать накопленные несистематизированные данные до информации, которая может быть охарактеризована как знания. Применительно к оценке качества ПЗ (ЗБ) для предобработки данных можно использовать подход, общая схема которого дана ниже.

3.1. Разбиение множества ОИ на классы типовых с точки зрения информационной безопасности объектов

На содержательном уровне задача разбиения ОИ на классы типовых объектов заключается в разбиении множества ОИ на непересекающиеся подмножества близких (в смысле существующих проблем информационной безопасности) объектов.

Решение данной задачи включает следующие этапы:

– категорирование защищаемой информации;

– определение множества характеристик (показателей) ОИ, существенных с точки зрения обеспечения информационной безопасности (определение пространства признаков $c_1, \ldots, c_p$ для классификации ОИ);

– построение разбиения на классы однотипных объектов на основе определения соответствующих функции близости и критерия разбиения на классы.

Для реализации первых двух этапов могут использоваться результаты, полученные в [5, 6], а для реализации третьего этапа – алгоритм последовательного разбиения ОИ либо эвристический алгоритм, аналогичные описанным в [6].

Результатом является построение разбиения вида

$$\bigcup_{i=1}^{n} K_i . \qquad (1)$$

К каждому из классов K_i, i=1, … ,n, относятся ОИ, у которых все признаки c_1, … ,c_w принимают одинаковые либо варьирующиеся в соответствующих допустимых диапазонах значения. Допустимый внутриклассовый разброс значений признаков определяется либо на основе субъективных экспертных критериев (в случае использования эвристического алгоритма), либо на основе формальных критериев, индуцируемых используемой формализованной процедурой разбиения. Для разных классов типовых ОИ определяются свои конкретные разбросы значений признаков. Например, класс ОИ может характеризоваться набором признаков {«уровень конфиденциальности обрабатываемой информации», «наличие контролируемой зоны», «выход во внешнюю сеть», «пользователи»} со следующими допустимыми значениями: {«информация ограниченного доступа», «открытая информация»}, «одна контролируемая зона», «выход во внешнюю незащищенную сеть», {«внутренние пользователи с разными правами доступа», «внешние пользователи с одинаковыми правами доступа»}.

Классу K_i, $1 \le i \le n$, ставится в соответствие эталонное описание вида

$$E_i = (\theta_{i1}, \ldots, \theta_{ip}), \qquad (2)$$

где θ_{ij} – множество допустимых значений показателя i, которые могут принимать ОИ из K_i.

3.2. Структурирование данных

Накапливаемый опыт структурируется по типам ОИ: собранные исходные данные разбиваются на n групп документов $\bigcup_{i=1}^{n} A_i$, соответствующих построенному разбиению (1). К группе A_i, $1 \le i \le n$, относятся документы, соответствующие объектам, входящим в класс K_i. Каждую группу A_i разбиваем на четыре подгруппы, соответствующие разным типам документов:

$$A_i = P_i \cup Z_i \cup G_i \cup Q_i, \tag{3}$$

где $P_i = \bigcup_{j=1}^{t(i)} P_{ij}$, $Z_i = \bigcup_{j=1}^{r(i)} Z_{ij}$, $G_i = \bigcup_{j=1}^{h(i)} G_{ij}$, $Q_i = \bigcup_{j=1}^{l(i)} Q_{ij}$ – подмножества ПЗ P_{ij}, $1 \le j \le t(i)$, ЗБ Z_{ij}, $1 \le j \le r(i)$, протоколов оценки ПЗ G_{ij}, $1 \le j \le h(i)$, и протоколов оценки ЗБ Q_{ij}, $1 \le j \le l(i)$, соответственно для ОИ, входящих в класс K_i.

Не исключено наличие классов K_i, для которых некоторые из множеств P_i, Z_i, G_i , Q_i являются пустыми. По мере последующего накопления опыта оценки множества P_i, Z_i, G_i , Q_i будут пополняться.

3.3. Фильтрация данных

Для каждого подмножества P_i, Z_i, G_i, Q_i, $I = 1, \ldots, n$, формируются эталоны $\Omega_i^{(P)}$ $\Omega_i^{(Z)}$, $\Omega_i^{(G)}$, $\Omega_i^{(Q)}$, характеризующие соответствующий тип документа для ОИ из K_i. Формирование эталонов позволяет исключить несущественную информацию и необходимость последующего неавтоматизированного анализа экспертом всей совокупности входящих в подгруппу документов, что существенно уменьшает трудоемкость процесса, а также влияние субъективного фактора.

3.3.1. Построение эталонов для однотипных ПЗ и ЗБ. Эталон $\Omega_i^{(P)}$ ($\Omega_i^{(Z)}$), $1 \le i \le n$, состоит из совокупности каталогов элементов безопасности ПЗ (ЗБ), описывающих возможные для ОИ из класса K_i:

– уязвимости безопасности $V(K_i) = \{v\}$ (каталог $C_i^{(P,V)}$ ($C_i^{(Z,V)}$));

– предположения безопасности $A(K_i) = \{a\}$ (каталог $C_i^{(P,A)}$ ($C_i^{(Z,A)}$));

– угрозы безопасности $Y(K_i) = \{y\}$ (каталог $C_i^{(P,Y)}$ ($C_i^{(Z,Y)}$));

– политики безопасности $L(K_i) = \{l\}$ (каталог $C_i^{(P,L)}$ ($C_i^{(Z,L)}$));

– задачи безопасности $G(K_i) = \{g\}$ (каталог $C_i^{(P,G)}$ ($C_i^{(Z,G)}$));

– требования безопасности $T(K_i,n) = \{t\}$ отдельно для каждого УГО, где n, $1 \le n \le 4$, – номер УГО (каталог $C_i^{(P,T,n)}$ ($C_i^{(Z,T,n)}$)). Каталог данного типа разбивается на четыре части: функциональные требования безопасности для объекта; функциональные требования безопасности для среды; требования безопасности для среды, не относящиеся к информационным технологиям, и гарантийные требования безопасности;

– средства безопасности $F(K_i,n) = \{f\}$ отдельно для каждого УГО и только для ЗБ (каталог $C_i^{(Z,F,n)}$);

– меры гарантии $M(K_i,n) = \{m\}$ отдельно для каждого УГО и только для ЗБ (каталог $C_i^{(Z,M,n)}$).

Указанные каталоги связаны между собой посредством следующей цепочки [7], соответствующей последовательности определения элементов безопасности при разработке ПЗ (ЗБ):

$$\begin{aligned}&\text{«}\textit{уязвимости} \rightarrow \{\textit{предположения, угрозы, политики}\} \rightarrow \textit{задачи безопасности} \rightarrow \\ &\rightarrow \textit{требования безопасности} \rightarrow \{\textit{средства безопасности, меры гарантии}\}\text{»}\end{aligned} \tag{4}$$

Отметим, что в отличие от работы [7] в последовательность (4) введен новый элемент безопасности «уязвимости». Это обусловлено тем, что без учета реально существующих уязвимостей объекта невозможно сформировать элементы безопасности ПЗ (ЗБ) вплоть до множества предъявляемых требований безопасности (и реализующих их средств безопасности и мер гарантии для ЗБ). В цепочке (4) элемент безопасности «уязвимости» служит отправной точкой, исходя из которой затем последовательно определяются остальные элементы.

Формирование каждого из каталогов сводится к следующим действиям:

– последовательному просмотру документов P_{ij}, $j = 1, \dots, t(i)$ (Z_{ij}, $j = 1, \dots, r(i)$) и включению в каталог формулировок соответствующих элементов безопасности (уязвимостей, предположений, угроз и др.), входящих хотя бы в один документ;

– выявлению и идентификации для каждого включенного в каталог элемента безопасности непосредственно связанных с ним элементов безопасности в соответствии с цепочкой (4), для чего используются сведения, приведенные в разделах «Обоснование ПЗ (ЗБ)» документов P_{ij} (Z_{ij}).

В итоге каталог $C_i^{(P,V)}$ ($C_i^{(Z,V)}$) состоит из совокупности кортежей вида

$$\tau_i^{(v)} = \langle v, A(v), Y(v), L(v)\rangle, \quad v \in V(K_i) = \bigcup_{j=1}^{t(i)} V_{ij} \quad (V(K_i) = \bigcup_{j=1}^{r(i)} V_{ij}),$$

где $A(v)$, $Y(v)$, $L(v)$ – множества предположений, угроз и политик, содержащихся в ПЗ (ЗБ) из P_i (Z_i) и направленных на предотвращение использования уязвимости v; V_{ij} – множество уязвимостей, приведенных в документе P_{ij} (Z_{ij}).

Каталог $C_i^{(P,A)}$ ($C_i^{(Z,A)}$) состоит из совокупности кортежей вида

$$\tau_i^{(a)} = \langle a, G(a)\rangle, \ a \in A(K_i) = \bigcup_{j=1}^{t(i)} A_{ij} \ (A(K_i) = \bigcup_{j=1}^{r(i)} A_{ij}),$$

где $G(a)$ – множество задач безопасности, содержащихся в ПЗ (ЗБ) из P_i (Z_i) и направленных на удовлетворение предположения a; A_{ij} – множество предположений, приведенных в документе P_{ij} (Z_{ij}).

Каталог $C_i^{(P,Y)}$ ($C_i^{(Z,Y)}$) состоит из совокупности кортежей вида

$$\tau_i^{(y)} = \langle y, G(y), B_Y(y)\rangle, \ y \in Y(K_i) = \bigcup_{j=1}^{t(i)} Y_{ij} \ (Y(K_i) = \bigcup_{j=1}^{r(i)} Y_{ij}),$$

где $G(y)$ – множество задач безопасности, содержащихся в ПЗ (ЗБ) из P_i (Z_i) и направленных на отражение угрозы y; Y_{ij} – множество угроз, приведенных в документе P_{ij} (Z_{ij}); $B_Y(y)$ – множество уязвимостей, обусловивших угрозу y.

Каталог $C_i^{(P,L)}$ ($C_i^{(Z,L)}$) состоит из совокупности кортежей вида

$$\tau_i^{(l)} = \langle l, G(l), B_L(l),\rangle, \ l \in L(K_i) = \bigcup_{j=1}^{t(i)} L_{ij} \ (L(K_i) = \bigcup_{j=1}^{r(i)} L_{ij}),$$

где $G(l)$ – множество задач безопасности, содержащихся в ПЗ (ЗБ) из P_i (Z_i) и направленных на обеспечение политики l; L_{ij} – множество политик, приведенных в документе P_{ij} (Z_{ij}); $B_L(l)$ – множество уязвимостей, обусловивших политику l.

Каталог $C_i^{(P,G)}$ ($C_i^{(Z,G)}$) состоит из совокупности кортежей вида

$$\tau_i^{(g)} = \langle g, T(g), B_G(g)\rangle, \ g \in G(K_i) = \bigcup_{j=1}^{t(i)} G_{ij} \ (G(K_i) = \bigcup_{j=1}^{r(i)} G_{ij}),$$

где $T(g)$ – множество требований безопасности, содержащихся в ПЗ (ЗБ) из P_i (Z_i) и направленных на решение задачи g; G_{ij} – множество задач, приведенных в документе P_{ij} (Z_{ij}); $B_G(g)$ – множество предположений, угроз и политик, обусловивших задачу g.

Каталог $C_l^{(P,T,n)}$ ($C_l^{(Z,T,n)}$) состоит из совокупности кортежей вида

$$\tau_l^{(t)} = \langle t, B_T(t)\rangle,\ t \in T(K_i,n) = \bigcup_{j=1}^{t(i,n)} T_{ij}^n;$$

$$(\tau_l^{(t)} = \langle t, F(t), M(t), B_T(t)\rangle,\ t \in T(K_i,n) = \bigcup_{j=1}^{r(i,n)} T_{ij}^n),$$

где $B_T(t)$ – множество задач безопасности, которые обусловили требование безопасности t; T_{ij}^n – множество требований безопасности, приведенных в документе P_{ij} (Z_{ij}) с заявленным УГО n; $F(t)$, $M(t)$ – множества наименований средств безопасности или мер гарантии соответственно, содержащихся в общей спецификации задания по безопасности Z_{ij} и направленных на реализацию требования t; T_{ij}^n – множество требований безопасности, приведенных в ЗБ Z_{ij} с заявленным УГО n; $t(i,n)$ ($r(i,n)$) – множество ПЗ (ЗБ) с заявленным УГО n, содержащихся в P_i (Z_i).

Каталог $C_l^{(Z,F,n)}$ состоит из совокупности кортежей вида

$$\tau_l^{(f)} = \langle f, B_F(f, n\rangle,\ f \in F(K_i,n) = \bigcup_{j=1}^{r(i,n)} F_{ij}^n,$$

где $B_F(f, n)$ – множество требований безопасности, содержащихся в ЗБ с заявленным УГО n, которые обусловили средство безопасности f; F_{ij}^n – множество средств безопасности, приведенных в ЗБ Z_{ij} с заявленным УГО n.

Каталог $C_l^{(Z,M,n)}$ состоит из совокупности кортежей вида

$$\tau_l^{(m)} = \langle m, B_M(m, n)\rangle,\ m \in M(K_i,n) = \bigcup_{j=1}^{r(i,n)} M_{ij}^n,$$

где $B_M(m, n)$ – множество требований безопасности, содержащихся в ЗБ с заявленным УГО n, которые обусловили меру гарантии m; M_{ij} – множество мер гарантии, приведенных в ЗБ Z_i с заявленным УГО n.

3.3.2. Построение эталонов для протоколов оценки однотипных ПЗ и ЗБ. Эталоны для групп документов вида G_i, Q_i, $1 \le i \le n$, состоят из совокупности описаний недостатков, обнаруженных ранее в ПЗ (ЗБ) для ОИ класса K_i. Недостатки структурируются по разделам, присутствующим в ПЗ (ЗБ) в соответствии с ISO/IEC 18045, т. е. разбиты на подгруппы недостатков, относящихся к разделам «Введение в описание ПЗ (ЗБ)», «Описание объекта», «Среда безопасности объекта», «Задачи безопасности», «Требования безопасности», «Дополнительные требования безопасности», «Общая спецификация» (только для ЗБ), «Обоснование ПЗ (ЗБ)», «Замечания по применению ПЗ» (только для ПЗ), «Требования соответствия ПЗ» (только для ЗБ).

Для каждого очередного раздела последовательно рассматривается совокупность протоколов G_{ij}, $j = 1, \dots, h(i)$ (Q_{ij}, $j = 1, \dots, l(i)$), в части, касающейся оценки данного раздела. В эталоны протоколов $\Omega_l^{(G)}$ ($\Omega_l^{(Q)}$) по каждому разделу вносятся все те недостатки, которые приведены хотя бы в одном из протоколов G_{ij}, $j = 1, \dots, h(i)$ (Q_{ij}, $j = 1, \dots, l(i)$):

$$\Omega_l^{(G)} = \bigcup_{q=1}^{8} \bigcup_{j=1}^{h(i)} S_{qji} \quad (\Omega_l^{(Q)} = \bigcup_{q=1}^{9} \bigcup_{j=1}^{l(i)} S_{qji}),$$

где S_{cji} – множество недостатков, зафиксированных по разделу c в протоколе G_{ij} (Q_{ij}) (в соответствии с приведенным выше перечнем ПЗ содержит восемь разделов, а ЗБ – девять).

Таким образом, в результате предобработки каждому классу K_i из разбиения (1) ставится в соответствие эталонное описание (2) входящих в него однотипных ОИ и четверка эталонных каталогов элементов безопасности и недостатков для ПЗ и ЗБ:

$$\langle \Omega_i^{(P)}, \Omega_i^{(Z)}, \Omega_i^{(G)}, \Omega_i^{(Q)} \rangle,$$

где $\Omega_i^{(P)} = \langle C_i^{(P,V)}, C_i^{(P,A)}, C_i^{(P,Y)}, C_i^{(P,L)}, C_i^{(P,G)}, \{C_i^{(P,T,n)}, n = 1, \dots, 4\}\rangle$, $\Omega_i^{(Z)} = \langle C_i^{(Z,V)}, C_i^{(Z,A)}, C_i^{(Z,Y)}, C_i^{(Z,L)}, C_i^{(Z,G)}, \{C_i^{(Z,T,n)}, n = 1, \dots, 4\}, \{C_i^{(Z,F,n)}, n = 1, \dots, 4\}, \{C_i^{(Z,M,n)}, n = 1, \dots, 4\}\rangle$.

4. Текущая актуализация опыта оценки

Ввиду непрерывного накопления все нового опыта оценки данные о нем должны постоянно пополняться и при необходимости корректироваться. Для этого можно использовать, например, подход, включающий следующие основные этапы:

– введение в состав исходных данных новых ПЗ, ЗБ и протоколов оценки в соответствии с формулами (1), (3);

– корректировку эталонов ПЗ, ЗБ и протоколов оценки с учетом новых данных и в соответствии с пп. 3.1 – 3.3. Предметом рассмотрения являются те подгруппы документов P_i, Z_i, G_i, Q_i, $1 \le i \le n$, которые были дополнены новыми документами.

Не исключено, что в процессе дальнейшего развития информационных технологий существующая классификация ОИ будет усовершенствована. В этом случае процедура предобработки исходных данных, приведенная в разд. 3, должна быть проведена заново.

5. Использование положительного опыта разработки ПЗ (ЗБ)

Пусть везде далее D – оцениваемый ПЗ (ЗБ) и O – ОИ, для которого он разработан. Предлагается следующий подход к использованию положительного опыта разработки ПЗ (ЗБ).

5.1. Классификация оцениваемого документа

Для ОИ O определяются, исходя из его специфики, значения $c_1(O),\dots,c_p(O)$ показателей, используемых в соответствии с п. 3.1 для классификации ОИ. ОИ O относится к тому классу K_i, $1 \le i \le n$, из разбиения (1), для которого в соответствии с (2) выполняется условие

$$c_1(O) \in \theta_{i1}, \dots, c_p(O) \in \theta_{ip}. \qquad (5)$$

Если условие (5) не выполняется ни для одного класса из (1), данное разбиение подвергается корректировке. Для этого производится экспертный анализ эталонов E_i, $i = 1, \dots, n$, с целью возможного уточнения и обновления диапазонов $\theta_{i1},\dots,\theta_{ip}$ допустимых значений показателей. Если после обновления эталонов (2) условие (5) станет выполняться для некоторого K_i, $1 \le i \le n$, то процесс завершается и ОИ O относится к данному классу. В противном случае разбиение (1) пополняется новым классом $K_{n+1} = \{O\}$, для которого определяется эталон E_{n+1}.

5.2. Оценка ПЗ (ЗБ) на основе сравнения с эталонными каталогами

Документ D сравнивается с эталонным образцом $\Omega_i^{(P)}$ ($\Omega_i^{(Z)}$) класса K_i, которому он принадлежит.

5.2.1. Последовательно просматриваются уязвимости, приведенные в каталоге уязвимостей $C_i^{(P,V)}$ ($C_i^{(Z,V)}$). Для каждой из них эксперт проверяет, действительно ли она имеет место для ОИ О, а также оценивает качество их описания в разделе «Описание объекта» документа D на основе сравнения с формулировками, приведенными в каталоге. Это позволяет выявить неучтенные или плохо определенные уязвимости, что помогает оценить полноту и качество описания уязвимостей в документе D.

5.2.2. Для каждой уязвимости *v*, приведенной в $C_i^{(P,V)}$ ($C_i^{(Z,V)}$) и включенной (либо подлежащей включению по результатам выполнения п. 5.2.1) в раздел «Описание объекта» документа *D*, рассматриваются предположения, угрозы и политики безопасности *A*(*v*), *Y*(*v*), *L*(*v*) из $\tau_i^{(v)}$. Оцениваются их наличие и качество изложения в *D* (на основе сравнения с формулировками из каталогов). Это позволяет выявить неучтенные либо плохо определенные предположения, угрозы и политики безопасности, что помогает оценить полноту и качество описания элементов среды безопасности в документе *D*.

5.2.3. Для каждых предположения *a*, угрозы *y* и политики безопасности *l*, приведенных в каталогах $C_i^{(P,A)}$, $C_i^{(P,Y)}$, $C_i^{(P,L)}$ ($C_i^{(Z,A)}$, $C_i^{(Z,Y)}$, $C_i^{(Z,L)}$) и включенных (либо подлежащих включению по результатам выполнения п. 5.2.2.) в раздел «Среда безопасности объекта» документа *D*, выделяются задачи безопасности *G*(*a*), *G*(*y*) и *G*(*l*) из $\tau_i^{(a)}$, $\tau_i^{(y)}$, $\tau_i^{(l)}$ соответственно. Оцениваются наличие данных задач и качество их формулировки в *D* (на основе сравнения с формулировками из каталогов). Это позволяет выявить неучтенные или плохо определенные задачи безопасности, что помогает оценить полноту и качество описания задач безопасности в документе *D*.

5.2.4. Для каждой задачи безопасности *g*, приведенной в каталоге $C_i^{(P,G)}$ ($C_i^{(Z,G)}$) и включенной (либо подлежащей включению по результатам выполнения п. 5.2.3.) в раздел «Задачи безопасности» документа *D*, выделяются требования безопасности *T*(*g*) из $\tau_i^{(g)}$. Оценивается их наличие и качество формулировки в *D* (на основе сравнения с формулировками из каталогов). Это позволяет выявить неучтенные или плохо определенные требования безопасности, что помогает оценить полноту и качество описания требований безопасности в документе *D*.

5.2.5. Если оцениваемый документ *D* является ЗБ с заявленным УГО *n*, $1 \le n \le 4$, то для каждого требования безопасности *t*, приведенного в каталоге $C_i^{(Z,T,n)}$ и включенного (либо подлежащего включению по результатам выполнения п. 5.2.4.) в разделы «Требования безопасности», «Дополнительные требования безопасности» либо «Гарантийные требования безопасности» документа *D*, выделяются реализующие его средства *F*(*t*) и меры *M*(*t*) из $\tau_i^{(t)}$. Оценивается их наличие и качество формулировки в *D* (на основе сравнения с формулировками из каталогов). Это позволяет выявить неучтенные или плохо определенные средства и меры гарантии, что помогает оценить полноту и качество описания общей спецификации в ЗБ *D*.

5.2.6. Для оценки качества обоснования, приведенного в документе *D*, последовательно рассматриваются все множества вида $B_Y(y)$, $B_L(l)$, $B_G(g)$, $B_T(t)$, $B_F(f,n)$, $B_M(m,n)$ из $\Omega_i^{(P)}$ ($\Omega_i^{(Z)}$). По результатам этих действий можно выявить неучтенные или плохо определенные аспекты обоснования, что помогает оценке полноты и качества обоснования в документе *D*.

Взаимозависимость элементов безопасности учитывается путем формирования множеств $B_Y(y)$, $B_L(l)$, $B_G(g)$, $B_T(t)$, $B_F(f,n)$, $B_M(m,n)$, обеспечивающих последовательность прямых импликативных связей на основе документов, уже прошедших успешную оценку; установления обратных импликативных связей на множестве элементов цепочки (4) по критерию связности. Здесь под связностью понимается критерий определения импликативной связи вида «если …, то» между элементами безопасности. Использование обратной импликативной связи исключает избыточность при определении элементов безопасности в соответствии с цепочкой (4).

6. Использование опыта о недостатках, допускаемых при разработке ПЗ (ЗБ)

Опыт о ранее выявленных недостатках накапливается в протоколах оценки $\Omega_i^{(G)}$ ($\Omega_i^{(O)}$), $i = 1, \dots, n$. Далее предлагается подход к его использованию.

6.1. Классификация оцениваемого документа

С помощью процедуры, описанной в п. 5.1, осуществляется классификация ОИ *O* относительно разбиения (1). Пусть *O* принадлежит классу K_i, $1 \le i \le n$.

6.2. Выбор эталонного протокола

Выбирается протокол $\Omega_i^{(G)}$, если оцениваемый документ D – ПЗ, и протокол $\Omega_i^{(Q)}$, если документ D – ЗБ.

6.3. Использование накопленного опыта о недостатках

Пусть $w_1, \dots, w_K$ – множество единиц работы, регламентированных стандартом для проведения оценки ПЗ (ЗБ) D. В процессе оценки эксперт должен выставить по каждой из них оценку $o(w_k,D)$, $k = 1, \dots, K$, отражающую качество выполнения требования безопасности, которое проверяется в рамках единицы работы w_k. Шкала оценок предложена в [4]. Ввиду того что выставление оценки полностью возлагается на эксперта, она весьма сильно зависит от субъективного фактора, что негативно влияет на ее адекватность. Учет апробированного накопленного опыта – эффективный способ решения данной проблемы.

Использование накопленного опыта при определении оценки $o(w_k, D)$ может состоять в следующем. Последовательно рассматриваются все недостатки, приведенные в $\Omega_i^{(G)}$ ($\Omega_i^{(Q)}$) для w_k. Для каждого из недостатков проверяется, имеет ли он место для документа D, что позволяет учесть оплошности, допускаемые ранее при разработке документов, аналогичных D. При выставлении оценки требуется обеспечить выполнение приведенных ниже условий.

Пусть $S(w_k,D,\Omega_i^{(G)})$ ($S(w_k,D,\Omega_i^{(Q)})$) – совокупность недостатков, отмеченных в $\Omega_i^{(G)}$ ($\Omega_i^{(Q)}$) для w_k и имеющих, по мнению эксперта, место для документа D. Тогда выставляемая оценка $o(w_k,D)$ должна удовлетворять условию

$$o(w_k, D) \le \min_{S(w_k,G_{ij}) \subseteq S(w_k,D,\Omega_i^{(G)}),\ 1 \le j \le h(i)} o(w_k,G_{ij}) \qquad \left(o(w_k, D) \le \min_{S(w_k,Q_{ij}) \subseteq S(w_k,D,\Omega_i^{(Q)}),\ 1 \le j \le l(i)} o(w_k,Q_{ij})\right),$$

где $S(w_k, G_{jj})$ ($S(w_k, Q_{jj})$) – совокупность замечаний, сделанных по единице работы w_k в протоколе G_{ij} (Q_{ij}); $o(w_k,G_{ij})$ ($o(w_k,Q_{ij})$) – оценка, выставленная по результатам выполнения w_k в G_{ij} (Q_{ij}).

Кроме того, если при вынесении оценки по единице работы w_k никаких новых недостатков, помимо перечисленных в протоколах из G_i (Q_j), не обнаружено, то оценка $o(w_k,D)$ должна удовлетворять также условию

$$o(w_k,D) \ge \max_{S(w_k,G_{ij}) \supseteq S(w_k,D,\Omega_i^{(G)}),\ 1 \le j \le h(i)} o(w_k,G_{ij}) \qquad \left(o(w_k,D) \ge \max_{S(w_k,Q_{ij}) \supseteq S(w_k,D,\Omega_i^{(Q)}),\ 1 \le j \le l(i)} o(w_k,Q_{ij})\right).$$

Заключение

Предложенный подход к использованию накопленного опыта предполагается реализовать в автоматизированной системе поддержки принятия решений при оценке ПЗ и ЗБ, разрабатываемой в лаборатории проблем защиты информации ОИПИ НАН Беларуси. Это позволит более эффективно использовать накопленный опыт оценки данных документов и тем самым даст возможность достигнуть более всестороннего анализа документов, повысить обоснованность принимаемых экспертных заключений, предоставить разработчику (в случае необходимости) конкретные конструктивные замечания по необходимой доработке ПЗ (ЗБ), создать необходимый базис для дальнейшего успешного испытания системы защиты ОИ.

Список литературы

1. Information technology and security Evaluation criteria for Information technology security. Part 3: Security assurance requirements : ISO/IEC 15408-3-1999. – 222 p.

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

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

4. 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.

5. Фисенко, В.К. Критерии классификации объектов информационных технологий по требованиям информационной безопасности / В.К. Фисенко, Е.П. Максимович // Комплексная защита информации : материалы IX Междунар. конф. – Минск : ОИПИ НАН Беларуси, 2005. – С. 103–105.

6. О некоторых подходах к категорированию объектов информатизации по требованиям информационной безопасности / В.В. Анищенко [и др.] // Комплексная защита информации : сб. науч. тр. – Минск : ОИПИ НАН Беларуси, 2000. – Вып. 3. – С. 5–22.

7. Захаревич, Н.С. Об опыте оценки качества профилей защиты и заданий по безопасности и практические рекомендации по разработке таких документов / Н.С. Захаревич [и др.] // Комплексная защита информации : материалы XIV Междунар. конф. – Минск : Донарит, 2009. – С. 100–103.

Поступила 08.04.10

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

U.V. Anishchanka, E.P. Maksimovich, O.V. Melekh, U.K. Fisenko

MATHEMATIC MODEL OF PROTECTION PROFILE AND SECUIRITY TARGET EVALUATION BASED ON ACCUMULATED EXPERIENCE

The formalized approach for using an expert’s experience for protection profile and security target evaluation is proposed. The evaluation is conducted in accordance with the Common Criteria. Implementation of the approach will increase the validity of expert decisions and may be used in automated decision making systems.