

## МЕТОДОЛОГИЯ СИНТЕЗА СИСТЕМ АНАЛИЗА И ОЦЕНКИ РИСКОВ ПОТЕРЬ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В работе представлено методологию синтеза систем анализа и оценки риска потерь информационных ресурсов, которая позволяет использовать широкий спектр параметров, дающая возможность создавать более гибкие средства анализа, а также оценивать риски, как на основе статистических данных, так и на экспертных оценках, сделанных в неопределенной, слабоформализованной среде с учетом периода времени, отрасли, экономической и управленческой специфики предприятия и др. Кроме этого, методология дает возможность отражать результаты как в качественной, так и в количественной форме, например, с использованием лингвистической переменной, часто применяемой для описания сложных систем.

Ключевые слова: риск, анализ риска, оценка риска, методология синтеза систем анализа и оценки риска, параметры риска.

Известно, что методологический базис является важнейшим компонентом теории защиты [3], который состоит из совокупности методов и моделей, необходимых и достаточных для исследований проблемы защиты и решения практических задач соответствующего назначения. В этой связи особого внимания заслуживают задачи анализа и оценки рисков (АОР) потерь информационных ресурсов (ИР). Однако, при практическом использовании существующих средств АОР [4, 5, 8] эксперты не всегда могут четко детерминировать оцениваемые параметры, поскольку их часто выражают в качественной форме. Поэтому, особый интерес представляют системы, которые позволяют эффективно проводить АОР (с учетом качественной и количественной оценки) в нечеткой, слабоформализованной среде. В связи с этим, целью данной работы является разработка соответствующей методологии синтеза систем АОР потерь ИР.

Используя известный подход [3] к построению методологий (синтеза систем оценки уровня безопасности информации в компьютерных системах, оценки систем технической защиты информации (ЗИ) на программно-управляемых АТС и выбора наилучшего варианта автоматическая телефонная станция (АТС) на базе интегрированной оценки уровня гарантий защищенности ИР), а также логико-лингвистический подход [3], предлагается (на основании разработанных методов [2] и модели интегрированного представления параметров рисков (ИППР) [1]) методология синтеза систем АОР потерь ИР (рис. 1). Она содержит двенадцать этапов: 1) выбор метода АОР; 2-5) идентификация ИР, действий, событий и оценочных компонент; 6-7) формирование степени риска (СР) и уровня оценочных компонент (УОК); 8-9) определение уровня значимости и текущего значения; 10) классификация текущих значений; 11-12) оценка и интерпретация СР. Теперь перейдем к более подробному описанию каждого из этапов.

**1. Выбор метода АОР.** На первом этапе для оценки СР эксперту необходимо осуществить выбор метода, в зависимости от среды в которой будет осуществляться АОР, а именно, основываясь на ситуации, когда у него имеются четкие (бинарные) предпочтения относительно значений оцениваемых параметров, так и на ситуации (с зоной его неуверенности) когда у эксперта присутствуют сомнения в однозначности своих приоритетов. В соответствии с этим методология позволяет проводить АОР потери ИР, как в детерминированной среде на основе применения DetM, так и в нечеткой – на основе FuzM [2]. В зависимости от осуществленного выбора (в дальнейшем на следующих этапах методологии) формируются интервалы значений, производится классификация текущих значений и осуществляется интерпретация полученных результатов.

**2. Идентификация информационных ресурсов.** На этом этапе для АОР осуществляется идентификация ИР. Для этого необходимо создать базу данных (БД) таких

ресурсов, после чего из нее экспертами производится выбор тех  $IP_h$   $h = \overline{1, r}$  (где  $h$  – указатель (номер) текущего идентификатора ИР, а  $r$  – количество ИР), которые характерны для объекта подвергающегося АОР, например, в результате прохождения этапа на выходе можем иметь следующие ИР:  $IP_1$  – “Сервер базы данных”,  $IP_2$  – “Принтер”,  $IP_3$  – “Сетевые файл-сервера” и т.п.

**3. Идентификация действий.** Этот этап подразумевает идентификацию возможных действий  $A \in \{A_a\}$  ( $a = \overline{1, n}$ ) (где  $a$  – указатель (номер) текущего идентификатора угрозы [1], а  $n$  – количество угроз), относительно каждого из идентифицированных на предыдущем этапе ИР. Для этого по аналогии с этапом 2, необходимо создать БД действий, из которой экспертами, производится выбор  $A_a$ , например, на выходе этапа при  $n=3$  для  $IP_1$  – “Сервер базы данных”, были идентифицированы, следующие  $A \in \{A_a\}$  ( $a = \overline{1, 3}$ ):  $A_1$  – “Аппаратные сбои и отказы”;  $A_2$  – “Диверсии”;  $A_3$  – “Перегрузки” и т.п.

**4. Идентификация событий.** Здесь необходимо идентифицировать события  $E \in \{E_e\}$  ( $e = \overline{1, 7}$ ) (где  $e$  – указатель (номер) текущего идентификатора события) нарушения информационной безопасности (ИБ), а именно на какие характеристики безопасности, каждого из ИР могут повлиять  $A_a$  идентифицированные на предыдущем этапе. В [6] определены три характеристики безопасности – конфиденциальность, целостность и доступность, в соответствии с этим в работе [1] при  $e=7$  были описаны идентификаторы базовых событий. В результате, на этом этапе получаем наборы  $IP_h, A_a, E_e$ , например, для  $IP_1$  идентифицированы  $A_1, A_2, A_3$ , которые могут привести соответственно к  $E_7$  – “НКЦД”,  $E_5$  – “НЦД”,  $E_3$  – “НД”.

**5. Идентификация оценочных компонент.** На этом этапе для создания возможности эксперту при оценивании использовать более широкий спектр величин, предлагается воспользоваться моделью ИППР [1]. Следовательно, для этого необходимо воспользоваться полным множеством оценочных компонент, которые могут использоваться при АОР –  $EK_{3Fh} \in \{EK_i\} = \{P, F, L, D, S, V\}$  ( $i = \overline{1, g}$ ,  $i$  – указатель (номер) текущего идентификатора оценочного компонента, а  $g$  – количество этих компонент) [2]. Например, при  $g=4$  ( $i = \overline{1, 4}$ ),  $EK_{3Ch} \in \{EK_i\} = \{EK_1, EK_2, EK_3, EK_4\} = \{P, F, L, D\}$  [2]. Результатом прохождения данного этапа является сформированное множество оценочных компонент, которое будет использоваться для АОР, а именно на этапах 8-10.

**6. Формирование эталонов для СР.** Этот этап предусматривает определение лингвистической переменной (ЛП) “СТЕПЕНЬ РИСКА” ( $DR$ ), соответствующей кортежу [3]

$\langle DR, T_{DR}, X_{DR} \rangle$ , для чего задается ее базовое терм-множество  $T_{DR} = \bigcup_{j=1}^m T_{DR_j}$  ( $j = \overline{1, m}$ , где  $m$

– количество термов), например, при  $m=3$  –  $\bigcup_{j=1}^3 T_{DR_j} = \{“Низкая”, “Средняя”, “Высокая”\}$ .

После определения термов необходимо задать универсальное множество  $X_{DR} \in \{0, \max_{DR}\}$ . Здесь, при условии выбора метода DetM, для каждого из термов  $T_{DR_1}, \dots, T_{DR_j}, \dots, T_{DR_m}$  задается свой интервал значений  $[dr_{min}; dr_1], \dots, [dr_m; dr_{max}]$ , а при выборе – FuzM, определяются эталонные нечеткие числа (НЧ) для  $DR$  относительно интервалов значений, количество которых зависит от числа используемых термов, например, если для  $DR$  их  $m$ , то количество интервалов будет  $G=2m-1$ , с общим видом  $[b_{11}; b_{21}], [b_{21}; b_{12}], [b_{12}; b_{22}], \dots, [b_{2m-1}; b_{1m}], [b_{1m}; b_{2m}]$  ( $j = \overline{1, m}$ ) и функцией принадлежности (ФП)  $\mu_j(dr)$  [3]. Сформированные интервалы, термы, НЧ и ФП в дальнейшем будут использоваться для интерпретации  $DR$  на этапе 12.

**7. Формирование эталонов для УОК.** Здесь, для определения УОК, формируется ЛП “УРОВЕНЬ ОЦЕНОЧНОГО КОМПОНЕНТА  $EK_i$ ” ( $K_{EK_i}$ ), которая определяется кортежем [3]  $\langle K_{EK_i}, T_{K_{EK_i}}, X_{K_{EK_i}} \rangle$ , где базовые терм-множества задаются  $m$  термами

$T_{K_{EK_i}} = \bigcup_{j=1}^m T_{K_{EK_{ij}}}$ , например, при  $m=3$  –  $\bigcup_{j=1}^3 T_{K_{EK_{ij}}} = \{\text{“Низкий”}, \text{“Средний”}, \text{“Высокий”}\}$ ,

которые в лингвистической форме характеризуют УОК и могут быть отображены на универсальное множество  $X_{EK_i} \in \{0, \max_{K_{EK_i}}\}$ . При выбранном DetM (см. этап 1), для  $T_{K_{EK_{i1}}}, \dots, T_{K_{EK_{im}}}$  соответственно задается свой интервал значений для каждого  $EK_i$  –  $[k_{EK_{i1} \min}; k_{EK_{i1}}[, \dots, [k_{EK_{im}}; k_{EK_{im} \max}]$ , а при – FuzM, осуществляется разбиение полного множества указанных значений на нечеткие подмножества, НЧ для  $K_{EK_i}$  можно отобразить относительно интервалов значений  $[b_{11}; b_{21}[$ ,  $[b_{21}; b_{12}[$ ,  $[b_{12}; b_{22}[$ , ...,  $[b_{2m-1}; b_{1m}[$ ,  $[b_{1m}; b_{2m}]$  ( $j = \overline{1, m}$ ) и ФП  $\mu_f(k_{EK_i})$ . Сформированные интервалы, термы, НЧ и ФП для УОР будут использоваться на этапе 10.

**8. Определение уровня значимости.** На этом этапе производится определение уровня значимости оценочных компонент. Здесь на основании  $\{EK_i\}$  (сформированном на 5 этапе) каждому компоненту ставится в соответствие уровень его значимости  $LS_i$  ( $i = \overline{1, g}$ ). Отметим, что если для всех  $LS$  справедливо отношение порядка (1) [2], то значимость  $i$ -го компонента определяется по правилу Фишберна (2) [2]. Если же все компоненты обладают равной значимостью (равнопредпочтительны т.е.  $LS_i = LS_{i+1}$  или системы предпочтений нет), то:  $LS_i = 1/g$  [2]. Полученные результаты определения  $LS_i$  будут использоваться на этапе 11.

**9. Определение текущего значения.** Здесь по каждому определенному на этапе 5 оценочному компоненту  $\{EK_i\}$  ( $i = \overline{1, g}$ ), с использованием сформированных на 7 этапе интервалов и термов  $K_{EK_i}$ , эксперты соответствующей предметной области определяют  $ek$  для всех  $A_a$  ( $a = \overline{1, n}$ ), идентифицированных на 3 этапе, т.е.  $\{ek_i^{A_a}\} = \{ek_P^{A_a}, ek_F^{A_a}, ek_L^{A_a}, ek_D^{A_a}, ek_S^{A_a}, ek_V^{A_a}\}$ . Значения выставляются на основании предпочтений экспертов, статистической информации и др. данных.

**10. Классификация текущих значений.** На этом этапе определяется принадлежность  $ek_i^{A_a}$  заданному интервалу (сформированному на 7 этапе). Далее формируется значение  $\lambda$  по формуле (4) и (9) для DetM и FuzM соответственно [2]. Аналогичные преобразования производятся для всех  $A_a$ . Исходящая информация используется на этапе оценки СР.

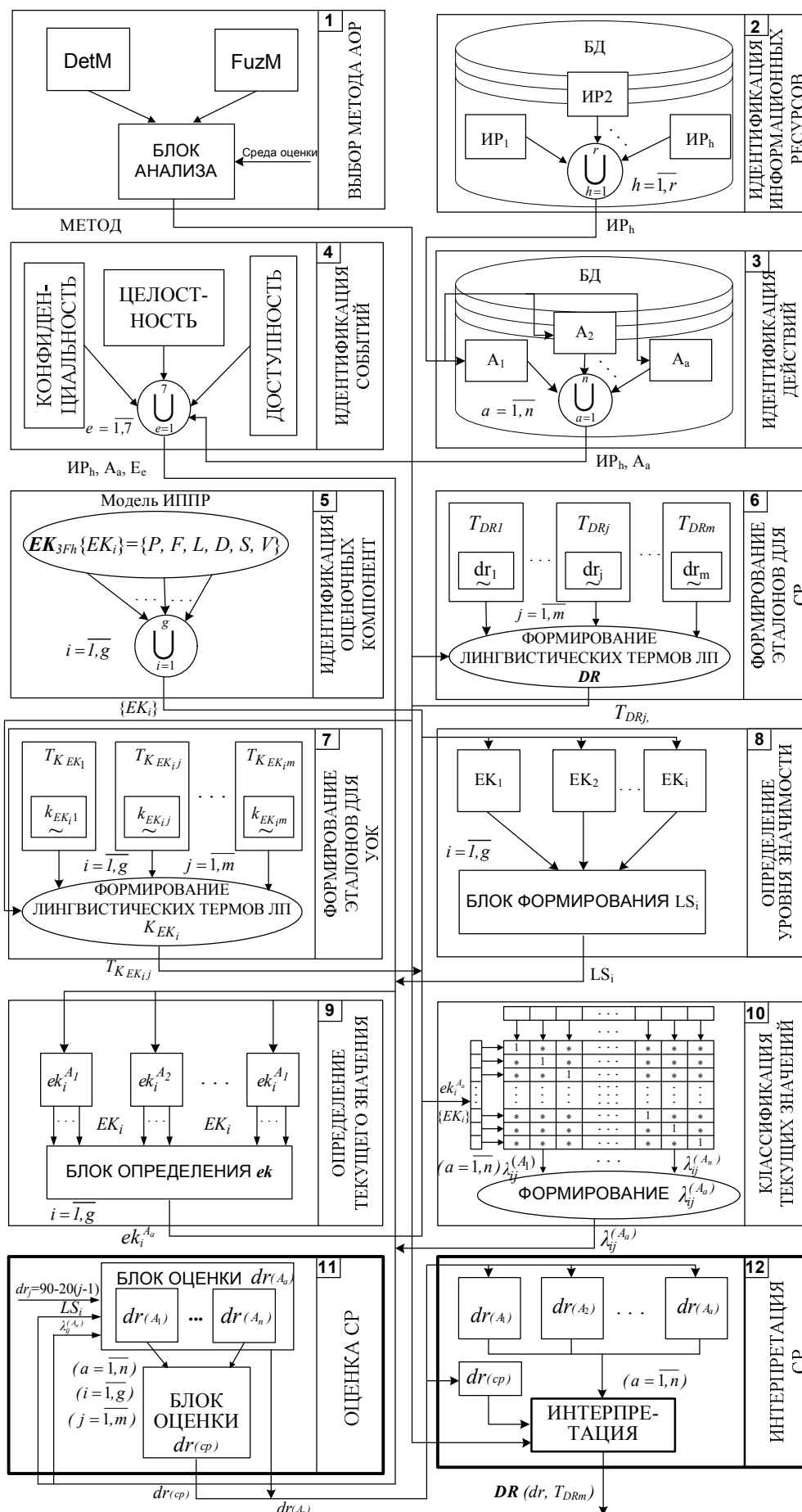


Рис. 1 Схема методологии синтеза систем анализа и оценки риска потерь ИР

**11. Оценка СР.** Здесь осуществляется оценка СР, для чего необходимо использовать наборы ИР<sub>h</sub>, A<sub>a</sub>, E<sub>e</sub>, LS<sub>i</sub> и  $\lambda_{ij}^{(A_a)}$ , которые формируются соответственно на этапах 4, 8 и 10. В дальнейшем по формуле (5) [2] (с вычислением  $dr_j=90-20(j-1)$ ) определяется показатель СР нарушения ИБ  $dr^{(A_a)}$  для каждого A<sub>a</sub> и его среднее значение  $dr^{(cp)}$  по ИР, с помощью выражения (7) [2].

**12. Интерпретация СР.** На этом этапе  $dr^{(A_a)}$  и  $dr^{(cp)}$  интерпретируются через определение соответствия измеренной СР определенным эталонным значениям, полученных на этапе 6, с помощью выражений (6) и (11) для DetM и FuzM соответственно [2]. Выходные данные, представляются как в лингвистической форме, так и в числовой.

Далее формируется отчет, в котором будут отражаться результаты 2 – 4, 9 – 12 этапов. Полученные данные в виде сформированного документа могут быть использованы при разработке модели угроз для различных классов информационных систем согласно требований [7] при построении комплексных систем защиты государственных информационных ресурсов, что в свою очередь даст возможность автоматизировать этот процесс.

На основании предложенной методологии можно строить как программные, так и программно-аппаратные системы, предназначенные для эффективного АОР потерь ИР, которые используют в качестве входных данных различные наборы оценочных параметров, что позволяет повысить гибкость и расширяет возможности проектируемых средств АОР функционирующих как в детерминированной, так и в нечетко определенной слабоформализованной среде.

## ЛІТЕРАТУРА

1. Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №1 (50). – С. 96 – 101.
2. Корченко А.Г. Методы анализа и оценки рисков потерь государственных информационных ресурсов / Корченко А.Г., Щербина В.П., Казмирчук С.В. // Защита информации – 2012. – №1. – С. 126-139.
3. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : “МК-Пресс”, 2006. – 320с. (ил. Монография).
4. Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности / Луцкий М.Г., Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации – 2011. – №3. – С. 97-108.
5. Луцкий М.Г. Современные средства управления информационными рисками / Луцкий М.Г., Иванченко Е.В., Корченко А.Г., Казмирчук С.В., Охрименко А.А. // Защита информации – 2012. – №1. – С. 5-16.
6. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТСЗІ СБ України від 28 квітня 1999 р. № 22.
7. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТСЗІ СБ України від 04 грудня 2000 р. № 53.
8. Скулыш Е.Д. Средства анализа и оценки риска информационной безопасности / Скулыш Е.Д., Корченко А.Г., Горбенко Ю.И., Казмирчук С.В. // Інформаційна безпека. Людина, суспільство, держава – 2011. – №3 (7). – С.31-48.

Надійшла: 10.04.2012

Рецензент: д.т.н., проф. Хорошко В.О.