DOI: 10.18372/2410-7840.19.11898
УДК 004.056.5

МЕТОДОЛОГИЯ СИНТЕЗА АДАПТИВНЫХ СИСТЕМ ОЦЕНИВАНИЯ РИСКОВ БЕЗОПАСНОСТИ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Александр Корченко, Светлана Казмирчук, Евгения Иванченко

На сегодня разработаны методы оценивания рисков (ОР) безопасности ресурсов информационных систем (РИС), которые не используются в едином методологическом базисе в разрезе стратегии исследований в области управления рисками и эффективного построения соответствующих систем информационной безопасности. В связи с этим, актуальной является задача разработки методологии синтеза систем ОР с учетом указанных методов. На основе известных исследований, а также логико-лингвистический подхода, предлагается усовершенствованная методология синтеза адаптивных систем ОР безопасности РИС, которая содержит десять этапов. Она, за счет введения дополнительных этапов (определения базовых параметров, выбор баз данных угроз/уязвимостей и РИС, формирование эталонов, выбор метода трансформирования термов, верификация лингвистических переменных), позволяет формализовать процесс создания адаптивных инструментальных средств с гибкими возможностями по обработке заданных множеств величин необходимых для ОР безопасности РИС.

Ключевые слова: *информационная безопасность, риск, оценивание рисков, методология синтеза систем, методологический базис, оценивания рисков безопасности ресурсов информационных систем.*

Известно, что методологический базис является важнейшим компонентом теории защиты информации [1], который состоит из совокупности методов и моделей, необходимых и достаточных для исследований проблемы защиты и решения практических задач соответствующего назначения. На сегодняшний день разработаны методы оценивания рисков (ОР) безопасности ресурсов информационных систем (РИС) [2-5], которые позволяют реализовать оценивание в детерминированных и нечетких условиях среды оценивания с участием и без участия экспертов соответствующей предметной области. Эти методы позволяют оперировать одновременно четкими и нечеткими параметрами с возможностью варьирования порядком лингвистической переменной (ЛП) [6, 7], а также реализовывать оперативное оценивание и мониторинг (в реальном времени) рисков без привлечения экспертов соответствующей предметной области [4, 5]. Для этого, например, можно использовать значения показателей информационной безопасности (ИБ) CVSS (версии 2.0 и 3.0), полученные на основании открытых баз данных уязвимостей (в качестве альтернативы оценок экспертов).

Сегодня известен методологический базис для синтеза следующих систем: оценивания уровня защищённости государственных ресурсов от социотехнических атак [7]; анализа состояния комплекса технической защиты информации [8]; выявления аномалий, порожденных кибератаками [9]; оценивания ущерба национальной безопасности в сфере охраны государственной тайны [10]; анализа и оценки рисков потерь информационных ресурсов [11] и т.д. Последняя методология связана с актуальной задачей ОР безопасности РИС. Однако, указанные выше методы и методология ОР не используются в единой стратегии исследований в области управления рисками и эффективного построения соответствующих систем ИБ. В связи с этим, актуальной является задача усовершенствования существующей методологии синтеза систем ОР ИБ [11].

Исходя из актуальности, целью данной работы является разработка соответствующей методологии синтеза адаптивных систем ОР безопасности РИС.

На основании известных исследований, связных с построением методологий [1], а также логико-лингвистический подхода [1], предлагается (на базе разработанных методов [[2]-5] и аналитико-синтетической кортежной модели характеристик риска (АСМ) [12]) усовершенствованная методология синтеза адаптивных систем ОР безопасности РИС (рис. 1). Она содержит десять этапов: 1) определение базовых параметров; 2) выбор метода ОР; 3) выбор БД РИС (БДРИС) и угроз/уязвимостей (БДУ/У); 4) идентификация РИС, угроз/уязвимостей; 5) формирование множества параметров ОР; 6) формирование эталонов; 7) выбор метода трансформирования термов; 8) верификация ЛП; 9) определение оценочных параметров (фаззификация); 10) оценивание и интерпретация СР (дефаззификация). Опишем более подробно каждый из этапов предложенной методологии.

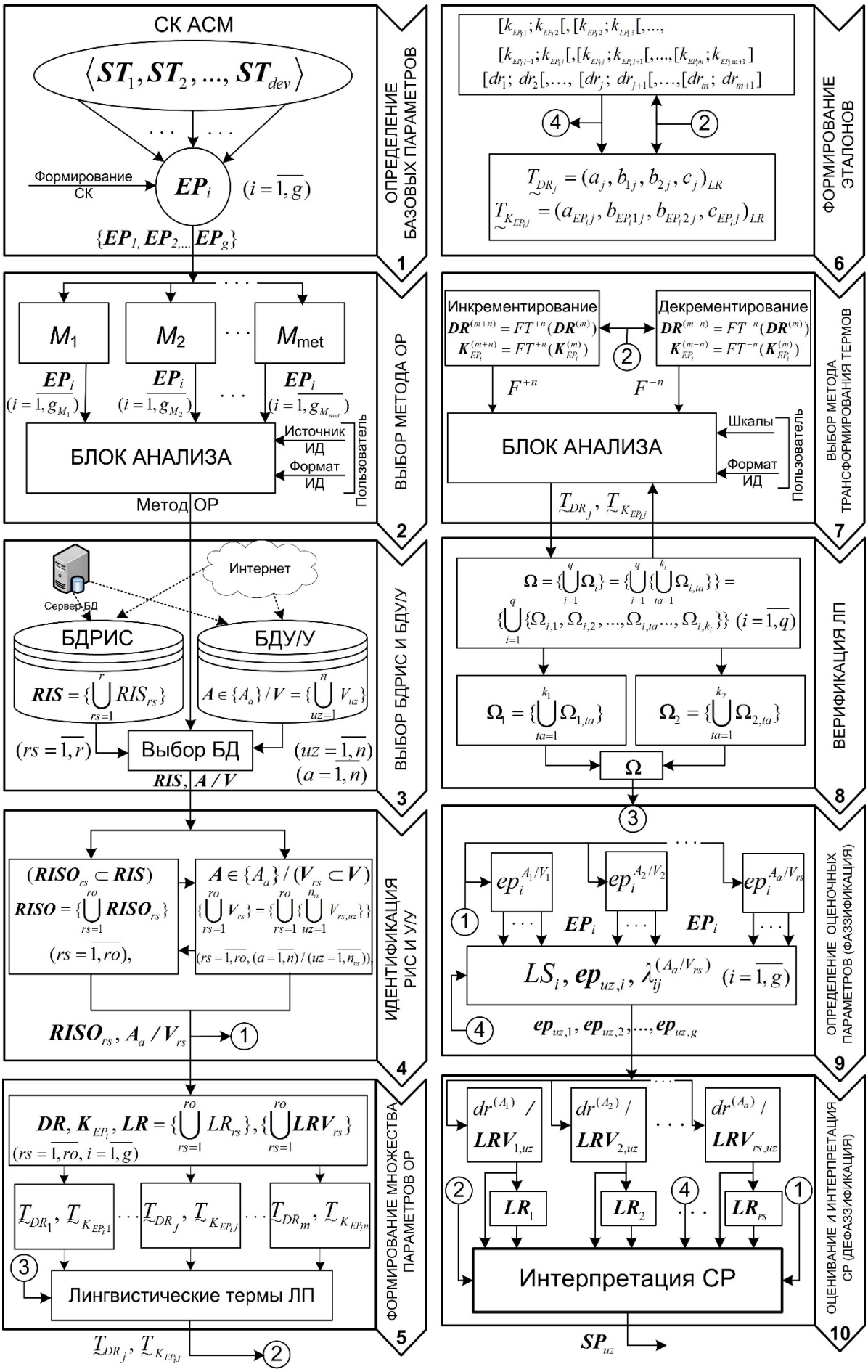

Рис. 1. Методология синтеза адаптивных систем оценивания рисков безопасности РИС

1. Определение базовых параметров. На первом этапе, для последующего оценивания СР, пользователю необходимо на основе синтетического кортежа (СК) $\langle \boldsymbol{ST}_1, \boldsymbol{ST}_2, ..., \boldsymbol{ST}_{dev} \rangle$ [12] посредством метода формирования СК [12] определить все необходимые базовые параметры, которые, по его мнению, должны использоваться при ОР. В результате реализации этого этапа формируются базовые множества параметров для ОР $\boldsymbol{EP}_i = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_g\}$ $(i = \overline{1, g})$.

2. Выбор метода ОР. Здесь, на основе сформированного на первом этапе множества $\boldsymbol{EP}_i$, пользователем осуществляется выбор метода ОР безопасности РИС в зависимости от источника и формата входных данных, определенных пользователем для дальнейшего ОР. К этим источникам относятся данные о возможных оценочных параметрах в СК. В соответствие с этим, методология позволяет производить ОР безопасности РИС на основе множества методов ОР M_{met} (где *met* – количество возможных методов ОР). Для каждого метода определяются оценочные параметры $\boldsymbol{EP}_i$ и их количество $(i = \overline{1, g_{M_1}}, i = \overline{1, g_{M_2}}, ..., i = \overline{1, g_{M_{met}}})$. Например, M_1 – интегрированный метод ОР [3], для которого при $i = \overline{1,4}$ $\boldsymbol{EP}_i$ может иметь вид $\boldsymbol{EP}_i = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3, \boldsymbol{EP}_4\} = \{\boldsymbol{D}, \boldsymbol{F}, \boldsymbol{L}, \boldsymbol{P}\}$ [2], M_2 – качественно-количественный метод ОР [4] и M_3 – метод ОР ИБ на основе открытых баз данных уязвимостей [5], где в качестве оценочных параметров могут использоваться $\boldsymbol{VA}$ (оценки CVSS) [4, 5, 13], а при $i = \overline{1,3}$ $\boldsymbol{EP}_i = \{\boldsymbol{EP}_1, \boldsymbol{EP}_2, \boldsymbol{EP}_3\} = \{\boldsymbol{B}, \boldsymbol{T}, \boldsymbol{E}\}$ и т.д. В зависимости от произведенного выбора (в дальнейшем на следующих этапах методологии) формируются соответствующие интервалы значений для ЛП.

3. Выбор БДРИС и БДУ/У. Здесь, в зависимости от выбранного (на 2 этапе методологии) метода ОР, осуществляется выбор БДРИС и БДУ/У, которые являются основой для определения всего множества $\boldsymbol{RIS} = \{\bigcup_{rs=1}^{r} RIS_{rs}\}$ $(rs = \overline{1, r})$ и угроз/уязвимостей (У/У) $\boldsymbol{A} \in \{A_a\} / \boldsymbol{V} = \{\bigcup_{uz=1}^{n} V_{uz}\}$ $(uz = \overline{1, n})$. В качестве таких БД могут служить, например, общедоступные (через интернет) БДУ/У [4] или БД, хранящиеся на соответствующих серверах и содержащие в себе, например, необходимые для реализации ОР статистические данные, полученные на предприятии за определенный промежуток времени.

4. Идентификация РИС и У/У. На этом этапе для ОР осуществляется идентификация РИС и У/У (в зависимости от выбранного метода ОР [3-5]). Для этого, согласно выбранного объекта оценивания, определяются множества РИС $\boldsymbol{RISO} = \{\bigcup_{rs=1}^{ro} \boldsymbol{RISO}_{rs}\}$ $(rs = \overline{1, ro})$ и У/У, т.е. $\boldsymbol{A} \in \{A_a\}$ $(a = \overline{1, n})$ / $\boldsymbol{V} = \{\bigcup_{rs=1}^{ro} \boldsymbol{V}_{rs}\} = \{\bigcup_{rs=1}^{ro} \{\bigcup_{uz=1}^{n_{rs}} V_{rs,uz}\}\}$ $(rs = \overline{1, ro},\ uz = \overline{1, n_{rs}})$ посредством соответствующих БД (множества определенных $\boldsymbol{RISO}_{rs} \subset \boldsymbol{RIS}$ и $\boldsymbol{V}_{rs} \subset \boldsymbol{V}$) [4, 5], выбранных на этапе 3 методологии. Например, в результате прохождения этого этапа на выходе можем получить следующие РИС: $\boldsymbol{RISO}_1$ = «Веб-сервер», $\boldsymbol{RISO}_2$ = «Операционная система», $\boldsymbol{RISO}_3$ = «Сетевой файл-сервер» и т.п., а при n=3 для $\boldsymbol{RISO}_1$ = «Веб-сервер» были идентифицированы следующие $\boldsymbol{A} \in \{A_a\}$ $(a = \overline{1,3})$: A_1= «Аппаратные сбои и отказы»; A_2= «Диверсии»; A_3= «Перегрузки».

5. Формирование множества параметров ОР. Этот этап ориентирован на определение множества всех ОР $\boldsymbol{LR}$ и $\boldsymbol{LRV}_{rs}$ $(rs = \overline{1, ro})$ [4], а также ЛП «СТЕПЕНЬ РИСКА» ($\boldsymbol{DR}$), соответствующей кортежу [1, 2, 4, 5] <$\boldsymbol{DR}$, $\underset{\sim}{T}_{DR}$, $\underset{\sim}{X}_{DR}$>. Для этого задается базовое терм-множество ЛП – $\underset{\sim}{T}_{DR} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{DR_j}$ ($j = \overline{1, m}$, где m – количество термов). Здесь также формируется ЛП «УРОВЕНЬ ОЦЕНОЧНОГО ПАРАМЕТРА $\boldsymbol{EP}_i$» ($\boldsymbol{K}_{EP_i}$), которая определяется кортежем [1, 2, 4, 5] < $\boldsymbol{K}_{EP_i}$, $\underset{\sim}{T}_{K_{EP_i}}$, $\boldsymbol{X}_{EP_i}$>, где базовые терм-множества определяются m термами $\underset{\sim}{T}_{K_{EP_i}} = \bigcup_{j=1}^{m} \underset{\sim}{T}_{K_{EP_i j}}$.

6. Формирование эталонов. Здесь, сформированным на этапе 5 ЛП $\boldsymbol{DR}$ и $\boldsymbol{K}_{EP_i}$, для каждого из термов $\underset{\sim}{T}_{DR_1}, \ldots, \underset{\sim}{T}_{DR_j}, \ldots, \underset{\sim}{T}_{DR_m}$ соответственно определяется свой интервал значений [dr_1; dr_2[, …, [dr_j; dr_{j+1}[,…, [dr_m; dr_{m+1}] ($j = \overline{1, m}$), а для $\underset{\sim}{T}_{K_{EP_i 1}}$, $\underset{\sim}{T}_{K_{EP_i 2}}$,…,

$\tilde{T}_{K_{EP_i j-1}}$, $\tilde{T}_{K_{EP_i j}}$, …, $\tilde{T}_{K_{EP_i m}}$ по каждому $\boldsymbol{EP}_i$ $(i=\overline{1,g})$ – $[k_{EP_i 1}; k_{EP_i 2}[, [k_{EP_i 2}; k_{EP_i 3}[, …, [k_{EP_i j-1}; k_{EP_i j}[, [k_{EP_i j}; k_{EP_i j+1}[, …, [k_{EP_i m}; k_{EP_i m+1}]$. Далее, с помощью метода [13] полученные интервалы преобразовываются в НЧ – $\tilde{T}_{DR_j}=(a_j; b_{1j}; b_{2j}; c_j)_{LR}$ и $\tilde{T}_{K_{EP_i j}} = (a_{EP_i j}, b_{EP_i 1 j}, b_{EP_i 2 j}, c_{EP_i j})_{LR}$. Сформированные интервалы значений, а также термы НЧ с ФП для УОП будут использоваться в качестве эталонов на этапе 10 при формировании структурированного параметра.

7. Выбор метода трансформирования термов. На 5 этапе осуществляется определение количества терм-множеств, которые будут использоваться в процессе ОР. При необходимости, пользователь, посредством этого этапа, осуществляет изменение начального порядка лингвистических эталонов без участия экспертов соответствующей предметной области. С этой целью для эквивалентного преобразования m-мерных термов НЧ ЛП $\boldsymbol{DR}^{(m)}$ в $\boldsymbol{DR}^{(m+n)} = FT^{+n}(\boldsymbol{DR}^{(m)})$ или $\boldsymbol{DR}^{(m-n)} = FT^{-n}(\boldsymbol{DR}^{(m)})$ и $\boldsymbol{K}_{EP_i}^{(m)} - \boldsymbol{K}_{EP_i}^{(m+n)} = FT^{+n}(\boldsymbol{K}_{EP_i}^{(m)})$ или $\boldsymbol{K}_{EP_i}^{(m-n)} = FT^{-n}(\boldsymbol{K}_{EP_i}^{(m)})$ предлагается воспользоваться методами инкрементирования или декрементирования порядка ЛП [6, 7]. После прохождения этого этапа в качестве выходных данных формируются преобразованные ЛП $\boldsymbol{DR}$ и $\boldsymbol{K}_{EP_i}$.

8. Верификация ЛП. Здесь, на базе преобразованных (на этапе 7) в процессе инкрементирования или декрементирования порядка ЛП $\boldsymbol{DR}$ и $\boldsymbol{K}_{EP_i}$, с помощью определенных аналитических выражений $\boldsymbol{\Omega} = \{\bigcup_{i=1}^{q} \boldsymbol{\Omega}_i\} = \{\bigcup_{i=1}^{q}\{\bigcup_{ta=1}^{k_i} \Omega_{i,ta}\}\} = \{\bigcup_{i=1}^{q}\{\Omega_{i,1}, \Omega_{i,2}, ..., \Omega_{i,ta}..., \Omega_{i,k_i}\}\}$ [14] и полученных новых термов $\tilde{T}_{DR_j}=(a_j; b_{1j}; b_{2j}; c_j)_{LR}$ и $\tilde{T}_{K_{EP_i j}} = (a_{EP_i j}, b_{EP_i 1 j}, b_{EP_i 2 j}, c_{EP_i j})_{LR}$, осуществляется верификация сформированных новых эталонов ЛП, которые в дальнейшем используются для ОР в качестве альтернативных значений начальных эталонов, определенных на этапе 5.

9. Определение оценочных параметров (фаззификация). На этом этапе производится определение уровня значимости оценочных параметров. Здесь, на основании $\boldsymbol{EP}_i$ (сформированном на 2 этапе) [4, 5], каждому параметру ставиться в соответствие уровень его значимости LS_i $(i=\overline{1,g})$. Полученные результаты определения LS_i будут использоваться на этапе 10 при оценивании СР. Также по каждому, определенному на этапе 2, оценочному параметру $\boldsymbol{EP}_i$ $(i=\overline{1,g})$, с использованием сформированных интервалов и термов $\boldsymbol{K}_{EP_i}$, эксперты соответствующей предметной области определяют $\boldsymbol{ep}_i$ для всех $\boldsymbol{A}_a/\boldsymbol{V}_{rs}$ $(a=\overline{1,n},\ rs=\overline{1,ro})$, идентифицированных на 4 этапе. Текущие значения оценочных параметров $\boldsymbol{ep}_i^{A_a/V_{rs}}$ формируются, например, на основании предпочтений экспертов, статистической информации, полученных CVSS метрик [4, 5] и др. данных (в зависимости от выбранного метода ОР на этапе 2). Далее, осуществляется процесс фаззификации, который связан с определением принадлежности $\boldsymbol{ep}_i^{A_a/V_{rs}}$ заданным интервалам значений ЛП $\boldsymbol{K}_{EP_i}^{(m)}$ и формированием значения $\lambda_{ij}^{(A_a/V_{rs})}$.

Аналогичные преобразования производятся для всех $\boldsymbol{A}_a/\boldsymbol{V}_{rs}$. Полученные данные LS_i и $\lambda_{ij}^{(A_a/V_{rs})}$ используются на этапе 10 при оценки СР.

10. Оценивание и интерпретация СР (дефаззификация). Здесь осуществляется оценка СР, для этого используются LS_i и $\lambda_{ij}^{(A_a/V_{rs})}$. Далее, по формуле (6), в [4] определяется показатель СР нарушения ИБ $\boldsymbol{dr}^{(A_a)}$ или $\boldsymbol{LRV}_{rs,uz}$ (в зависимости от выбранного метода ОР на 2 этапе) для каждого $\boldsymbol{A}_a/\boldsymbol{V}_{rs}$ и с помощью выражения (8) в [4] его среднее значение $\boldsymbol{dr}^{(\phi)}$ или $\boldsymbol{LR}_{rs}$ по РИС. Затем осуществляется процесс дефаззификации, который связан с формированием структурированного параметра СР SP_{uz} с помощью формулы (9) в [4], позволяющий получить числовые значения $\boldsymbol{dr}^{(A_a)}/LRV_{rs,uz}$ и $\boldsymbol{dr}^{(\phi)}/\boldsymbol{LR}_{rs}$, а также их лингвистическую интерпретацию. Выходные данные представляются, как в лингвистической форме, так и в числовой. Далее, формируется отчет, в котором будут отражаться результаты основных процессов, выполненных на этапах 4 - 10.

Таким образом, усовершенствована методология синтеза адаптивных систем оценивания рисков безопасности РИС, в которой, за счет введения дополнительных этапов (определения базовых параметров, выбор БДРИС и БДУ/У, формирование эталонов, выбор метода трансформирования термов, верификация ЛП), позволяет фор-

мализовать процесс создания адаптивных инструментальных средств с гибкими возможностями по обработке заданных множеств величин при оценивании рисков безопасности РИС.

Полученные данные в виде сформированного документа могут быть использованы при построении систем менеджмента информационной безопасности или комплексных систем защиты информации.

На основании предложенной методологии можно строить как программные, так и программно-аппаратные системы, предназначенные для эффективного ОР безопасности РИС, которые используют в качестве входных данных различные наборы оценочных параметров, что позволяет обеспечить гибкость, адаптивность и расширение функциональных возможностей проектируемых средств ОР, реализующих оценивание, как в детерминированной, так и в нечетко определенной слабоформализованной среде.

ЛИТЕРАТУРА

[1]. А. Корченко, *Построение систем защиты информации на нечетких множествах. Теория и практические решения*, К.: МК-Пресс, 2006, 320 с.

[2]. А. Корченко, А. Архипов, С. Казмирчук, *Анализ и оценивание рисков информационной безопасности. Монография*, Киев: ООО «Лазурит-Полиграф», 2013, 275 с.

[3]. С. Казмирчук, А. Гололобов, "Интегрированный метод анализа и оценивания рисков информационной безопасности", *Захист інформації*, Т. 16, №3, С. 252-261, 2014.

[4]. А. Корченко, С. Казмирчук, "Качественно-количественный метод оценивания рисков информационной безопасности", *Захист інформації*, Т. 18, №2, С. 157-170, 2016.

[5]. А. Корченко, С. Казмирчук, "Метод оценивания рисков информационной безопасности на основе открытых баз данных уязвимостей", *Безпека інформації*, №2, С. 216-226, 2016.

[6]. А. Корченко, Б. Ахметов, С. Казмирчук, Н. Сейлова, А. Гололобов, "Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков", *Захист інформації*, Т. 16, №4, С. 284-291, 2014.

[7]. А. Корченко, Б. Ахметов, С. Казмирчук, М. Жекамбаева, "Метод n-кратного инкрементирования числа термов лингвистических переменных в задачах анализа и оценивания рисков", *Безпека інформації*, Т. 21, №2, С. 191-200, 2015.

[8]. Г. Баранов, М. Захарова, Д. Горніцька, "Методологія синтезу систем оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак", *Захист інформації*, Т. 14, №3, С. 98-104, 2012.

[9]. Б. Журиленко, "Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома", *Захист інформації*, Т. 17, №3, С. 196-204, 2015.

[10]. А. Корченко, В. Щербина, Н. Вишневская, "Методология построения систем выявления аномлий порожденных кибератаками", *Захист інформації*, Т. 18, №1, С. 30-38, 2016.

[11]. О. Корченко, М. Луцький, М. Захарова, Ю. Дрейс, "Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці", *Захист інформації*, Т. 15, №1, С. 14-20, 2013.

[12]. Е. Иванченко, С. Казмирчук, А. Гололобов, "Методология синтеза систем анализа и оценки рисков потерь информационных ресурсов", *Захист інформації*, Т. 14, №2, С. 24-28, 2012.

[13]. А. Корченко, С. Казмирчук, Ю. Дрейс, А. Гололобов, "Бистабильная интегрированная кортежная модель характеристик риска", *Защита информации*, №4, С. 314-323, 2016.

[14]. А. Корченко, С. Казмирчук, "Метод преобразования интервалов в нечеткие числа для систем анализа и оценивания рисков", *Правовое, нормативное и метрологическое обеспечение системы защиты информации в Украине*, № 1(31), С. 57-64, 2016.

[15]. А. Корченко, Ф. Приставка, Б. Ахметов, С. Казмирчук, "Аналитические выражения верификации лингвистических переменных для систем оценивания рисков информационной безопасности", *Безпека інформації*, №1, С. 50-55, 2017.

REFERENCES

[1]. A. Korchenko *The construction of security systems on the fuzzy sets. Theory and practical solutions*, 2006, 320 p.

[2]. A. Korchenko, S. Kazmirchuk, A. Arkhipov, *The analysis and assessment risks information security. Monograph*, 2013, 275 p.

[3]. S. Kazmirchuk, A. Gololobov, " The integrated risk analysis and risk assessment method of information security ", *Zahist ìnformacìï,* no. 3, pp. 252-261, 2014.

[4]. A. Korchenko, S. Kazmirchuk, "The qualitative and quantitative method of information security risk assessment", *Zahist ìnformacìï*, no. 2, pp. 157-170, 2016.

[5]. A. Korchenko, S. Kazmirchuk, "The risk assessment method of information security based on open databases vulnerabilities", *Bezpeka informatsiyi*, no. 2, pp. 216-226, 2016.

[6]. A. Korchenko, B. Akhmetov, S. Kazmirchuk, A. Gololobov, N. Seylova, "The n-fold decrease method of terms number of linguistic variables in risk assessment and task analysis, *Zahist ìnformacìï*, vol. 16, no. 4, pp. 284-291, 2014.

[7]. A. Korchenko, B. Akhmetov, S. Kazmirchuk, M. Zhakambayeva, "Method of n-fold incrementa-tion the number of terms the linguistic variables in the tasks of

analysis and risk assessment", *Bezpeka informatsiyi*, vol. 21 no. 2, pp. 191-200, 2015.
[8]. G. Baranov, M. Zaharova, D. Gornicka, "Methodology for the synthesis of systems security level evaluation of public information resources from social engineering attacks", *Zahist ìnformacìï*, vol. 14, no. 3, pp. 98-104, 2012.
[9]. B. Zhurilenko, "Construction and analysis methodology of complex technical information security with probabilistic reliability and counting of temporal breaking attempts", *Zahist ìnformacìï*, vol. 17, no. 3, pp. 196-204, 2015.
[10]. A. Korchenko, V. Shcherbyna, N. Vyshnevska, "A methodology for building cyberattack-generated anomaly detection systems", *Zahist ìnformacìï*, vol. 18, no. 1, pp. 30-38, 2016.
[11]. O. Korchenko, M. Lutskii, M. Zaharova, Y. Dreis, "Synthesis methodology and software implementation system evaluation harm to national security in protection of state secrets", *Zahist ìnformacìï*, vol. 15, no. 1, pp. 14-20, 2013.
[12]. E. Ivanchenko, S. Kazmirchuk, A. Gololobov, "The methodology for synthesis of risk analysis and assessment systems of information resources loss", *Zahist ìnformacìï*, vol. 14, no. 2, pp. 24-28, 2012.
[13]. A. Korchenko, S. Kazmirchuk, Y. Dreis, A. Gololobov, "Bistable and integrated based tuple model of risk characteristics", *Zahist ìnformacìï*, no. 4, pp. 314-323, 2016.
[14]. A. Korchenko, S. Kazmirchuk, "Method of intervals transformation in fuzzy numbers for information security risk analysis and assessment systems", *Legal, regulatory and metrological support of information security in Ukraine*, no. 1(31), pp. 57-64, 2016.
[15]. A. Korchenko, P. Prystavka, S. Kazmirchuk, B. Akhmetov, "Analytical verification expressions of linguistic variables for information security risk assessment systems", *Bezpeka informatsiyi,* no. 1, pp. 50-55, 2017.

МЕТОДОЛОГІЯ СИНТЕЗУ АДАПТИВНИХ СИСТЕМ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

На сьогодні розроблені методи оцінювання ризиків (ОР) безпеки ресурсів інформаційних систем (РІС), які не використовуються в єдиному методологічному базисі в розрізі стратегії досліджень в галузі управління ризиками і ефективної побудови відповідних систем інформаційної безпеки. У зв'язку з цим, актуальним є завдання розробки методології синтезу систем ОР з урахуванням зазначених методів. На основі відомих досліджень, а також логіко-лінгвістичного підходу, пропонується вдосконалена методологія синтезу адаптивних систем ОР безпеки РІС, яка містить десять етапів. Вона, за рахунок введення додаткових етапів (визначення базових параметрів, вибір баз даних загроз/уразливостей та РІС, формування еталонів, вибір методу трансформування термів, верифікація лінгвістичних змінних), дозволяє формалізувати процес створення адаптивних інструментальних засобів з гнучкими можливостями з обробки заданих множин величин необхідних для ОР безпеки РІС.

Ключові слова: інформаційна безпека, ризик, оцінювання ризиків, методологія синтезу систем, методологічний базис, оцінювання ризиків безпеки ресурсів інформаційних систем.

THE METHODOLOGY FOR THE SYNTHESIS OF ADAPTIVE RISK ASSESSMENT SYSTEMS OF SECURITY INFORMATION SYSTEM RESOURCES

Today, the methods of risk assessment (RA) of security information system resources (ISR) have been developed, which are not used in a single methodological basis in the context of research strategy in the field of risk management and the effective construction of appropriate information security systems. In this regard, the actual task is to develop methods for the synthesis of RA systems, taking into account these methods. On the basis of well-known studies, as well as the logical-linguistic approach, an improved methodology for the synthesis of adaptive RA systems of security (ISR), which contains ten stages, is proposed. It, through the introduction of additional stages (base parameters definition, selection of databases threats/vulnerabilities and ISR, formation of standards, a choice of terms transformation method, verification of linguistic variables), allows to formalize the creation process of adaptive tools with flexibility for processing the specified sets of values required for RA of security ISR.

Keywords: information security, risk, risk assessment, methodology for the synthesis systems, methodological basis, risk assessment of security information system resources.

Корченко Александр Григорьевич, доктор технических наук, профессор, лауреат Государственной премии Украины в области науки и техники, заведующий кафедрой безопасности информационных технологий Национального авиационного университета, визит-профессор Университета в Бельско-Бялой (Гуманитарно-техническая академия в Бельско-Бялой, г. Бельско-Бяла, Польша), ведущий научный сотрудник Национальной академии СБ Украины.
E-mail: icaocentre@nau.edu.ua
Корченко Олександр Григорович, доктор технічних наук, професор, лауреат Державної премії України в галузі науки і техніки, завідувач кафедри безпеки інформаційних технологій Національного авіаційного університету, візит-професор Університету в Бельсько-Бялій (Гуманітарно-технічна академія в Бельсько-Бялій, м. Бельсько-Бяла, Польща), провідний науковий співробітник Національної академії СБ України.

Korchenko Oleksandr, Dr Eng (Information security), professor, laureate of the State Prize of Ukraine in Science and Technology, Head of IT-Security Academic Department, National Aviation University, Visit-Professor at The University of Bielsko-Biala (Akademia Techniczno-Humanistyczna, Bielsko-Biała, Poland), Leading Researcher of the National Academy of SS of Ukraine.

Казмирчук Светлана Владимировна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: sv.kazmirchuk@gmail.com
Казмірчук Світлана Володимирівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Kazmirchuk Svitlana, PhD in Eng., Associate Professor of IT-Security Academic Department, National Aviation University.

Иванченко Евгения Викторовна, кандидат технических наук, доцент, профессор кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: evivancenko@gmail.com
Іванченко Євгенія Вікторівна, кандидат технічних наук, доцент, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Ivanchenko Eugenia, PhD in Eng., Professor of IT-Security Academic Department, National Aviation University.

DOI: 10.18372/2410-7840.19.11899
УДК 004.056.53

ПРИМЕНЕНИЕ РЕФЛЕКСИВНЫХ МОДЕЛЕЙ РИСКОВ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ В КИБЕРПРОСТРАНСТВЕ

Александр Архипов

Рассматриваются возможности и границы применения риск-ориентированного подхода (РОП) к построению и исследованию системы защиты информации организации (СЗИ). Введены четыре вербальных спецификации злоумышленника, описывающие различные аспекты его поведения и подготовки, социально-психологический контекст его действий, целевые установки этих действий, влияющие на выбор стратегии злоумышленника, методы и способы реализации информационных угроз. Соответственно введенным спецификациям сформированы рефлексивные модели рисков. Это математические модели, структура и параметры которых отражают (лат. reflexus) особенности злоумышленника, содержащиеся в его спецификации. Выполнено исследование рефлексивных моделей, которое в ряде случаев позволило определить предельные объёмы инвестиций в СЗИ, а также ограничения в применении РОП к построению СЗИ.
Ключевые слова: *риск, моделирование рисков, рефлексивные модели рисков, предельные объёмы инвестиций в СЗИ, риск-ориентированный подход.*

В основе большинства наиболее часто и успешно применяемых международных и отраслевых стандартов для систем менеджмента безопасности информации (СМБИ): ISO 27001, ISO 27005, СТО БР ИББС, NIST SP 800-30, COSO ERM-Integrated Framework и т.д., лежит риск-ориентированный подход (РОП), обеспечивающий получение определенных преимуществ в построении и эксплуатации СМБИ.

В частности, в отличие от директивного подхода к построению систем защиты информации (СЗИ), базирующегося на использовании рекомендованного перечня возможных угроз в отношении доступности, целостности и конфиденциальности информации, как правило в полном объёме привлекаемого для формирования системы услуг безопасности при построении СЗИ, РОП позволяет из огромного количества существующих угроз и уязвимостей информационных систем (ИС) выделить те, которые действительно актуальны для защиты информации в данной конкретной организации, что создает объективные предпосылки минимизации инвестиций в безопасность информации. Детальный анализ механизмов реализации выделенного ограниченного