DOI: 10.18372/2410-7840.19.11443
УДК 004.056.5

ИССЛЕДОВАНИЕ СРЕДСТВ ОЦЕНИВАНИЯ РИСКОВ БЕЗОПАСНОСТИ РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ

Филипп Приставка, Петр Павленко, Светлана Казмирчук, Марина Коломиец

Одним из основных этапов построение комплексных систем обеспечения безопасности ресурсов информационных систем является оценивания рисков. Часто перед специалистами компаний для повышения эффективности решения задач защиты информации возникает вопрос о выборе адекватного средства оценивания рисков информационной безопасности, которое будет удовлетворять соответствующие требования. На сегодня существует достаточно широкое множество таких средств. Для их рационального выбора проведено исследование множества средств оценивания рисков с целью определения набора необходимых сравнительных характеристик. Относительно указанных средств с учетом известной аналитико-синтетической кортежной модели характеристик риска формируется кортеж, который дает возможность относительно определенных параметров унифицировать процесс сравнительного анализа таких средств. Это повысит эффективность осуществления их выбора для решения соответствующих задач информационной безопасности.
Ключевые слова: *информационная безопасность, риск, оценивание рисков, аналитико-синтетическая кортежная модель, средств оценивания рисков информационной безопасности, угроза, уязвимость, характеристики риска.*

Одним из главных этапов комплексного подхода к построению систем защиты информации ресурсов информационных систем (РИС) является оценивания рисков. Сегодня существует достаточно широкое множество средств оценивания рисков (СОР) информационной безопасности (ИБ), при выборе которых перед специалистами возникает ряд вопросов, например: «Какие используются входные величины для оценивания?», «Какой математический аппарат используется для оценивания?», «В какой среде (условиях) реализуется оценивание?» и т.д. В работе [1] была предложена аналитико-синтетическая кортежная модель характеристик риска (АСМ), основанная на двух кортежах – аналитическом (АК) (который используется для исследования широкого спектра существующих средств оценивания рисков с позиций формирования необходимых для их функционирования исходных данных) и синтетическом (который используется для помощи разработчикам, синтезирующих соответствующие средства оценивания). Эта модель позволяет упростить принятие решения о выборе необходимого средства оценивания и определение необходимого набора параметров для создания систем оценивания рисков.

В [7, 8] проводился анализ наиболее известных СОР с использованием кортежной модели интегрированного представления параметров риска. Этот подход дал возможность относительно такой модели, унифицировать процесс исследования соответствующих СОР и обеспечить рациональность осуществления их выбора. Кортежная модель интегрированного представления параметров риска была усовершенствована за счет ввода множеств интегрированных характеристик рисков, подмножеств их идентифицирующих и оценочных компонент, отраженных в отношении определенных критериев аналитическим и синтетическим кортежами [1]. Также по отношению к исследованиям, проведенных в [7, 8], появились новые методы и средства, для которых подобный анализ не проводился. В связи с этим, актуальной является задача исследования существующих СОР с использованием усовершенствованной АСМ.

Исходя из актуальности, целью данной работы является расширенное исследование дополнительных СОР (с использованием предложенного в [1] подхода) для определения используемых наборов характеристик, по которым можно осуществить сравнительный анализ указанных средств. Это повысит эффективность решения соответствующих задач в области ИБ.

В качестве исходных средств исследования, были взяты следующие СОР – Coras, Ebios, ISAMM, $IRAM_2$ и PTA.

Метод Coras (разработан в рамках программы Information Society Technologies Европейского союза (SINTEF ICT, Норвегия), используется для анализа рисков безопасности критически важных систем и реализуется посредством технологии UML (Unified Modeling Language – унифицированный язык моделирования). Ориентирована на поддержку требований стандартов AS/NZS 4360: 1999 (Risk Management) и ISO/IEC 17799-1: 2000 (Code of Practice for Information Security Management). Средство оценивания (метод) основывается на восьми шагах [2] (см. рис. 1). Шаг 1 – сбор общей информации об объекте анализа. Шаг 2 – определение цели, направления и масштаба анализа. Шаг 3 – детализация

задач анализа (см. рис. 2). Шаг 4 – анализ и изучение полученной документации; Шаг 5 – определение рисков на основе метода «мозгового штурма». Шаг 6 – определение уровня рисков, оценивание вероятностей для угроз (сценариев угроз) и последствий инцидентов ИБ (см. рис. 3). Шаг 7 – определение приемлемых и неприемлемых рисков. Шаг 8 – определение процедур для устранения угроз с целью уменьшения возможной вероятности (последствий инцидентов) в области ИБ. Шаги 1-4 являются подготовительными, поскольку здесь аналитики собирают информацию об объекте анализа, формируют его цели и шкалы для определения величины вероятности и последствий (см. табл. 1 и 2), а также критерии оценивания рисков (см. табл. 3).

Таблица 1

Пример вероятностной шкалы

Значение вероятности	**Описание**	**Определение**
Точно	Пять и более раз в год	[50; ∞⟩ : 10 лет = [5; ∞ ⟩ : 1 год
Вероятно	От двух до пяти раз в год	[20; 50⟩ : 10 лет = [2; 5⟩ : 1 год
Возможно	Менее чем 2 раза в год	[5; 20⟩ : 10 лет = [0,5; 2⟩ : 1 год
Вряд ли	Меньше чем 1 раз в 2 года	[1; 5⟩ : 10 лет = [0,1; 0,5⟩ : 1 год
Редко	Меньше чем 1 раз в 10 лет	[0; 1⟩ : 10 лет = [0; 0,1⟩ : 1 год

Далее это будет использоваться для идентификации последних. Шаги 5-8 предназначены для анализа и непосредственно определения рисков, их уровней (см. табл. 3), выявления и оценивания потенциальных возможностей уменьшения неприемлемых рисков [2].

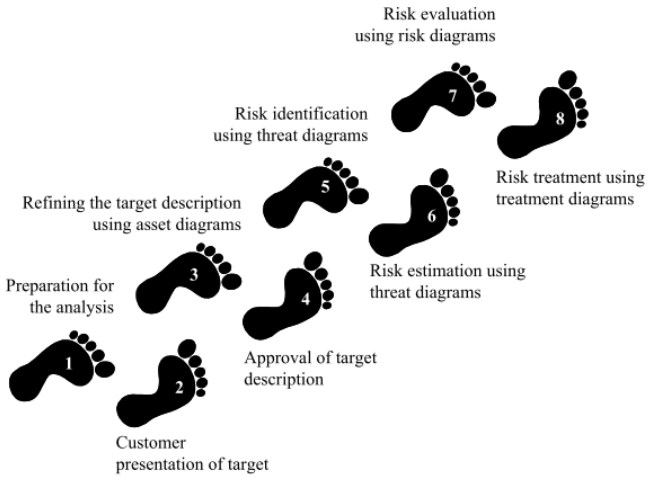

Рис. 1. Восемь шагов метода Coras

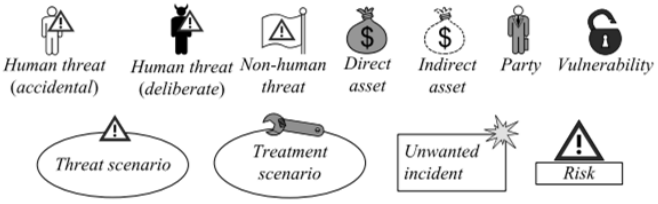

Рис. 2. Примеры символов для моделирования риска

Таблица 2

Пример шкалы последствий

Значение последствия	**Количество ресурсов***
Катастрофическое	>1000
Большое	101÷1000
Среднее	11÷100
Низкое	1÷10
Незначительное	0
*ресурсы, подвергающиеся воздействию	

Таблица 3

Пример матрицы оценки риска

Вероятность	**Последствие**				
	Незначительное	Низкое	Средние	Большое	Катастрофическое
Редко			CC1, CC1(I)		
Вряд ли					PR1
Возможно		CI1(I), SS1(I)	CI1, SS1		
Вероятно				SS2	
Точно					

CC1, CC1(I) – компрометация конфиденциальности, а (I) показывает, что ресурс косвенный;
CI1, CI1(I) – компрометация целостности; SS1, SS1(I) – замедление системы;
SS2 – невозможность работать из-за зависания системы; PR1 – получения неправильных данных.

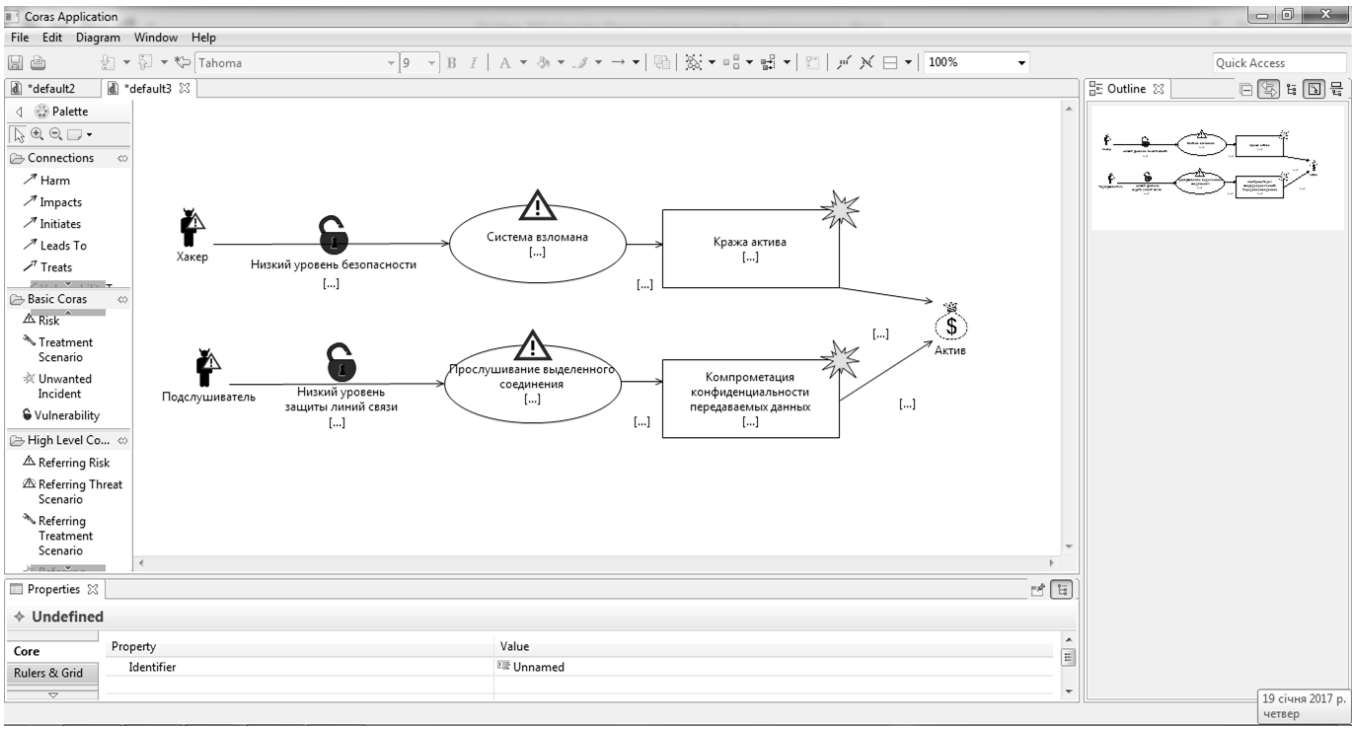

Рис. 3. Пример интерфейса инструментария Coras
(первоначальная схема угроз для умышленных действий)

Относительно характеристик риска [1] для метода Coras можно получить отображение компонент ***P***, ***D*** и ***V(A)***. Элемент ***P***, исходя из указанного примера (см. табл. 1-3), отображается вероятностью реализации угрозы ***V(A)***, а последствия можно косвенно представить в виде элемента ***D***. Также из табл. 4 видно, что все угрозы приводят к нарушению различных характеристик безопасности и могут быть связаны со значением E_7 = «НКЦД». Все расчеты отображаются в качественных и количественных шкалах, что можно отразить через элемент M_3.

Анализ показал, что прямого использования компонентов ***D***, ***E*** и ***M*** в системе нет, но прослеживается с ними логическая связь, поэтому эти величины являются косвенными. Здесь и далее для обозначения косвенных характеристик в кортеже будет использоваться символ *, например, ***D****. После проведенного анализа с учетом АСМ [1] АК, отображающий этот метод можно представить в виде **<*E**, *D**, *M**, *P*, *V(A)*>**.

Метод EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité, разработчик Национальное агентство компьютерной безопасности (ANSSI), Центральное управление безопасности информационных систем (DCSSI), Франция) отображает требования стандартов ISO/IEC 27001, ISO 31000 и ISO/IEC 27005. Процесс анализа и оценивания риска реализуется посредством пяти модулей.

Модуль 1 – исследование контекста. Здесь реализуется сбор информации об объекте оценивания посредством трех мероприятий. Мероприятие 1 – определение сферы управления рисками. Мероприятие 2 – подготовка метрик (критерии безопасности (табл. 4), уровни опасности (табл. 5) и вероятности (табл. 6) и критерии управления рисками). Мероприятие 3 – идентификация РИС [3].

Модуль 2 – исследование нежелательных событий. Здесь реализуется определение важных РИС (с точки зрения доступности, целостности, конфиденциальности) и всех угроз, которые могут привести к нарушению безопасности (их источники и вероятности).

Модуль 3 – исследование сценариев угроз, который ориентирован на выявление и оценку сценариев, что могут вызвать описанные события, отражающие риски. С этой целью исследуются источники угроз и уязвимости.

Модуль 4 – исследование рисков. Здесь непосредственно оцениваются риски реализации сценариев угроз, исследованных в модуле 3.

Модуль 5 – исследование мер безопасности. Пятый модуль ориентирован на определение мер безопасности и реализацию их тестирования [3].

Таблица 4

Пример критериев безопасности

Критерии безопасности	Определения	Шкала уровня	Подробное описание шкалы
Доступность	Доступность РИС, своевременность РИС первой необходимости	]72 ч; ∞[	РИС не доступны более 72 часов
		]24 ч; 72 ч]	РИС доступны в течении 72 часов
		]4 ч; 24 ч]	РИС доступны в течении 24 часа
		]0 ч; 4 ч]	РИС доступны в течении 4 часов
Целостность	Точность и полнота основных РИС	Выявляемые	Изменения РИС идентифицируются
		Определенные	Изменения РИС идентифицируются и определяются (локализируются)
		Целостные	Изменения РИС не осуществляются
Конфиденциальность	Основные РИС доступны только зарегистрированным пользователям	Открытые	Публичные
		Ограниченные	Доступ только для сотрудников и партнёров
		Служебные	Доступ имеют только персонал, который участвует в разработке
		Персонализированные	Доступ только для конкретных лиц

Таблица 5

Пример шкалы опасности

Шкала уровня	Описание
1. Незначительная	Преодоление последствий без каких-либо трудностей
2. Средняя	Преодоление последствий несмотря на ряд трудностей
3. Высокая	Преодоление последствий с серьезными трудностями
4. Критическая	Непреодолимые последствия

Относительно АСМ с учетом [1] для EBIOS определим АК. Так компонентам $\boldsymbol{D}$ и $\boldsymbol{P}$ (исходя из указанного примера шкалы для опасности и вероятности) соответствуют, например, значения для D_1= «Незначительная», D_2= «Средняя», D_3= «Высокая», а для P_1= «Минимальная», P_2= «Средняя», P_3= «Высокая» и т.д.

Также рассматриваются уязвимости и угрозы $\boldsymbol{V(A)}$, которые приводят к нарушению определенных характеристик ИБ, атакованных РИС, и соответственно связываются со значениями E_3= «НД», E_1= «НК», E_2= «НЦ». Анализ показывает, что $\boldsymbol{M}$ принимает значение M_1, а с учетом АСМ, АК для этого метода можно представить в виде $\boldsymbol{<E, D, M^*, P, V(A)>}$.

Таблица 6

Пример вероятностной шкалы реализации сценариев угроз

Шкала уровня	Описание
1. Минимальная	Не должно произойти
2. Средняя	Может произойти
3. Высокая	Возможно или точно произойдет через день-два
4. Максимальная	Произойдет в ближайшее время

Метод ISAMM (Information Security Assessment & Monitoring Method, разработчик Telindus S.A. (Security, Audit and Governance Services, Бельгия) основан на требованиях стандарта ISO/IEC 27002. Он основывается на трех базовых компонентах: анализ объекта, оценка риска, отчетность. Этот количественный метод оценивания рисков ИБ отображает их через ежегодные ожидаемые убытки в денежных единицах (Annual Loss Expectancy (ALE)). На первых этапах работы с методом определяются угрозы ИБ (см. табл.7) [4].

При оценке риска для каждой угрозы (T) оценивается вероятность ее появления – p_T и ожидаемые последствия – I_T. Ежегодные ожидаемые убытки ALE_T для конкретной угрозы T определяются произведением вероятности возникновения и воздействия угрозы: $ALE_T = p_T \cdot I_T$ (см. табл. 8). Также вычисляется сумма $ALE = \sum_T ALE_T$ по объекту оценивания [4].

Относительно АК отметим, что все угрозы $\boldsymbol{V(A)}$ приводят к нарушению ИБ $\boldsymbol{E}$ (см. табл. 8). Относительно оценивания риска в методе используют элементы $\boldsymbol{L}$ и $\boldsymbol{P}$, которые отображаются ежегодными ожидаемыми убытками и вероятностью реализации угроз, а воздействие можно косвенно отобразить как $\boldsymbol{D^*}$. Относительно элемента $\boldsymbol{M}$ следует отметить, что метод использует количественные шкалы, то соответствует M_2. С учетом этого АК для этого метода можем представить в виде: $\boldsymbol{<E, D^*, L, M^*, P, V(A)>}$.

Таблица 7

Пример идентифицированных угроз

ХИБ	ИУ	Описание
К	С1	Внешние злоумышленники получили или получат доступ к конфиденциальной информации
К	С2	Внутренние злоумышленники получили или получат доступ к конфиденциальной информации
К	С3	Случайное раскрытие конфиденциальных данных внутренними злоумышленниками
К	С4	Случайное раскрытие конфиденциальных данных внешними злоумышленниками
Ц	І1	Модификация или повреждение внешними злоумышленниками
Ц	І2	Модификация или повреждение внутренними злоумышленниками
Ц	І3	Случайная, ошибочная модификация
Д	А1	Отказ в обслуживании или другие нарушения, вызванные злоумышленниками (вредоносным кодом)
Д	А2	Нехватка ресурсов, ноу-хау, поддержка поставщика
Д	А3	Стихийные бедствия (землетрясения, наводнения, ураганы, молнии, пожар, экстремальные погодные условия), террористические или промышленные (ударные) воздействия
Д	А4	Отключение системы на короткий период, например, из-за погодных условий
Д	А5	Непреднамеренные отключения из-за ошибок

ХИБ – характеристика ИБ; ИУ – идентификатор угрозы;
К – конфиденциальность; Ц – целостность; Д – доступность.

Таблица 8

Пример оценивания рисков

Угроза	Вероятность (в год)	Воздействие (€)	Текущие ALE_T (€)
С1	1	2000	2000
С2	0,2	2000	400
С3	0,5	400	200
С4	0,5	2000	1000
І1	0,2	50000	10000
І2	0,04	50000	2000
І3	0,5	400	200
А1	0,2	10000	2000
А2	0,2	400	80
А3	0,1	10000	1000
А4	2	400	800
А5	0,5	2000	1000
	Всего	129600	20680

Методология IRAM₂ (Information Risk Assessment Methodology 2, разработчик Форум информационной безопасности (Information Security Forum), США) реализуется с помощью шести этапов. Этап 1 – обзор (связан с реализацией анализа рисков). Этап 2 – оценка воздействия (определение и оценка различных категорий воздействий на бизнес). Этап 3 – профиль угрозы (разрабатывается модель угроз). Этап 4 – оценка уязвимостей (выявление возможностей среды/системы насколько хорошо она может противостоять угрозам). Этап 5 – оценивание риска (определяется соотношение вероятности реализации угрозы и величины ее воздействия (рис. 4)). Этап 6 – обработка риска (реализуется разработка планов обработки рисков) [5].

Отметим, что в данном COP идентифицируются как угрозы, так и уязвимости ***V(A)***, которые могут быть связаны с событиями (***E***) нарушения базовых характеристик ИБ. Исходя из этого, характеристика ***E**** в методологии присутствует косвенно. Касательно других элементов, то при оценке риска используется вероятность ***P*** и воздействие, которое можно косвенно отобразить посредством ***D****. После проведенного анализа АК для этой методологии имеет следующий вид: **<*E**, *D**, *M**, *P*, *V(A)*>**.

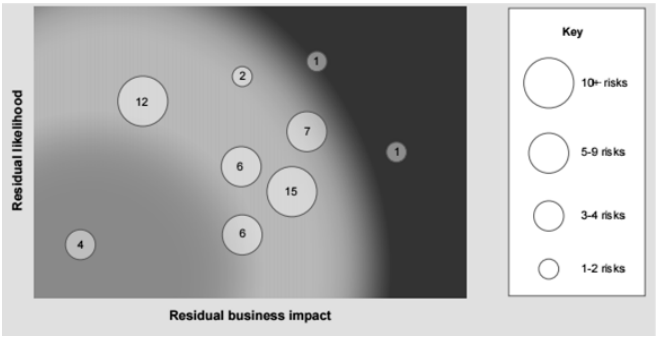

Рис. 4. Пример отображения риска

Инструментарий PTA (Practical Threat Analysis, разработчик PTA Technologies, Израиль) основан на требованиях стандарта ISO/IEC 27001 и PCI DSS 1.1. Представляет собой программную систему для разработки модели угроз, оценивания рисков ИБ и составления планов по их снижению. Все перечисленные процессы реализуются посредством четырех шагов.

Шаг 1 – определение РИС. Здесь реализуется идентификация РИС с указанием их стоимости, связанных с ними угроз, процентное соотношение от общей стоимости всех РИС системы. Также каждому ресурсу присваивается идентификатор, например, А003 (см. рис. 5) [6].

Шаг 2 – выявление уязвимостей. На этом шаге анализируются и фиксируются все уязвимости (рис. 6) и угрозы, к которым они могут привести. Также здесь реализуется оценивание рисков как соотношение вероятности реализации угрозы и ущерба от ее реализации (рис. 7) [6].

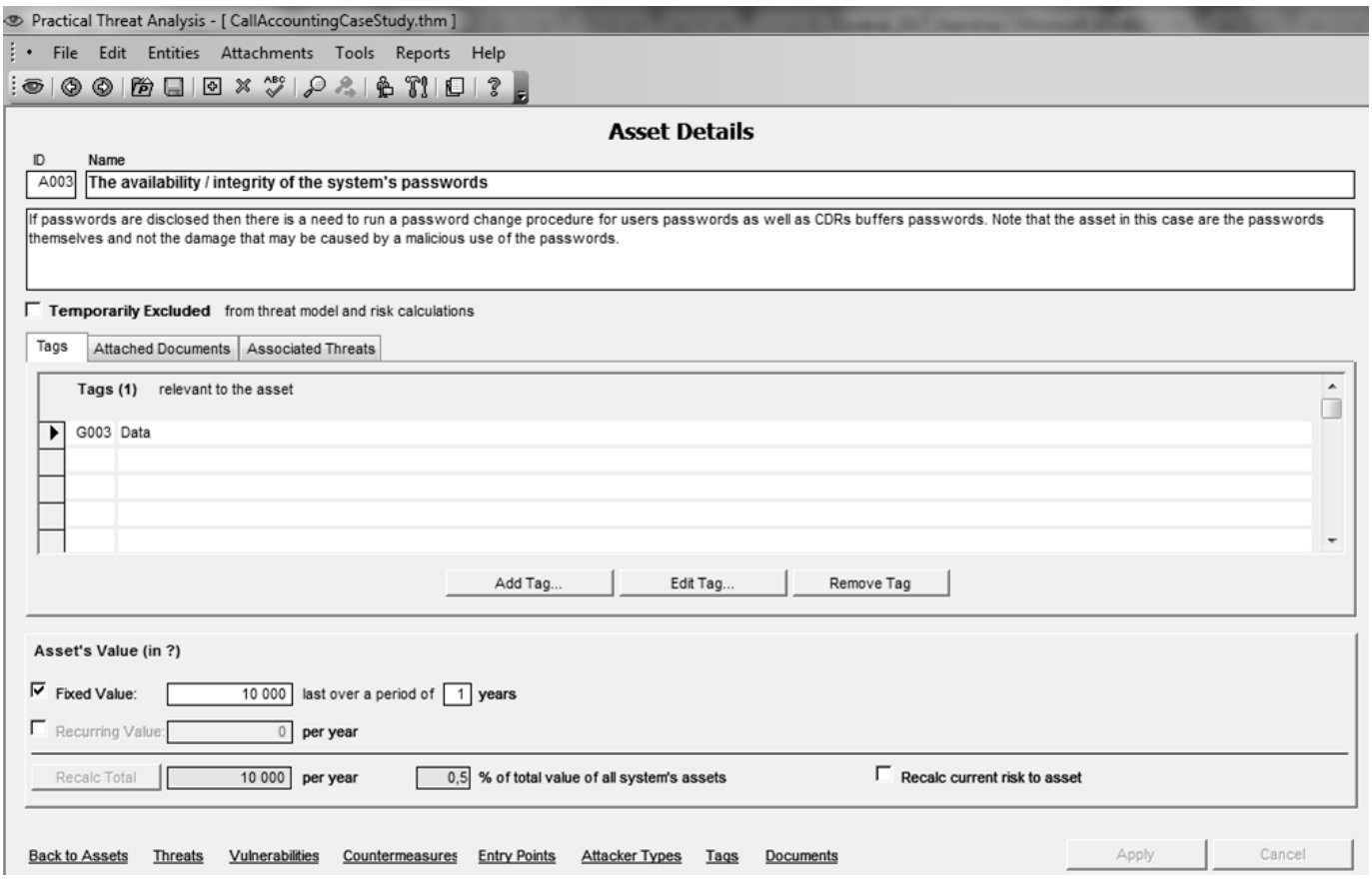

Рис. 5. Пример формы для идентификации РИС

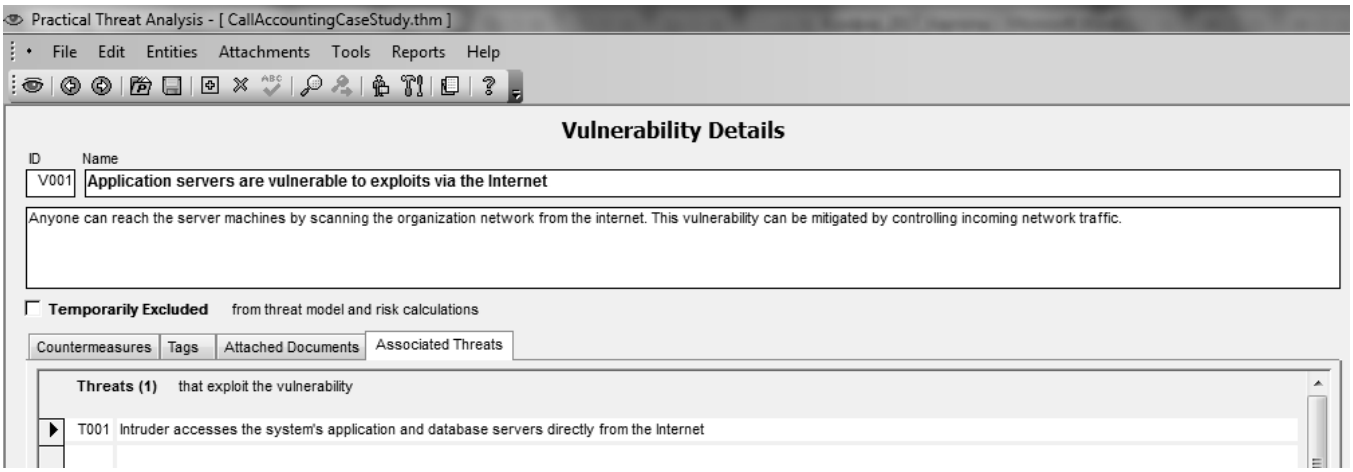

Рис. 6. Пример формы для фиксирования уязвимостей

Шаг 3 – определение контрмер. Этот шаг подразумевает выбор контрмер для перекрытия уязвимости и предотвращения реализации угроз (см. рис. 7 и 8).

Шаг 4 – разработка планов нейтрализации сценариев угроз (рис. 9) [6].

Относительно АК определим кортеж для этого инструментария. Элемент ***V(A)*** отображается уязвимостями и угрозами (см. рис. 6 и 7), которые могут привести к нарушению характеристик ИБ, так, например, V_1 = «Серверы приложений уязвимы для эксплойтов через Интернет» может привести к E_1 = «НК». Для оценки риска в инструментарии используются элементы ***P***, ***L*** и косвенно ***D****, который отображает значение параметра «Повреждения» (см. рис. 7).

Следовательно, АК для РТА имеет вид: ***<E*, D*, L, M*, P, V(A)>***.

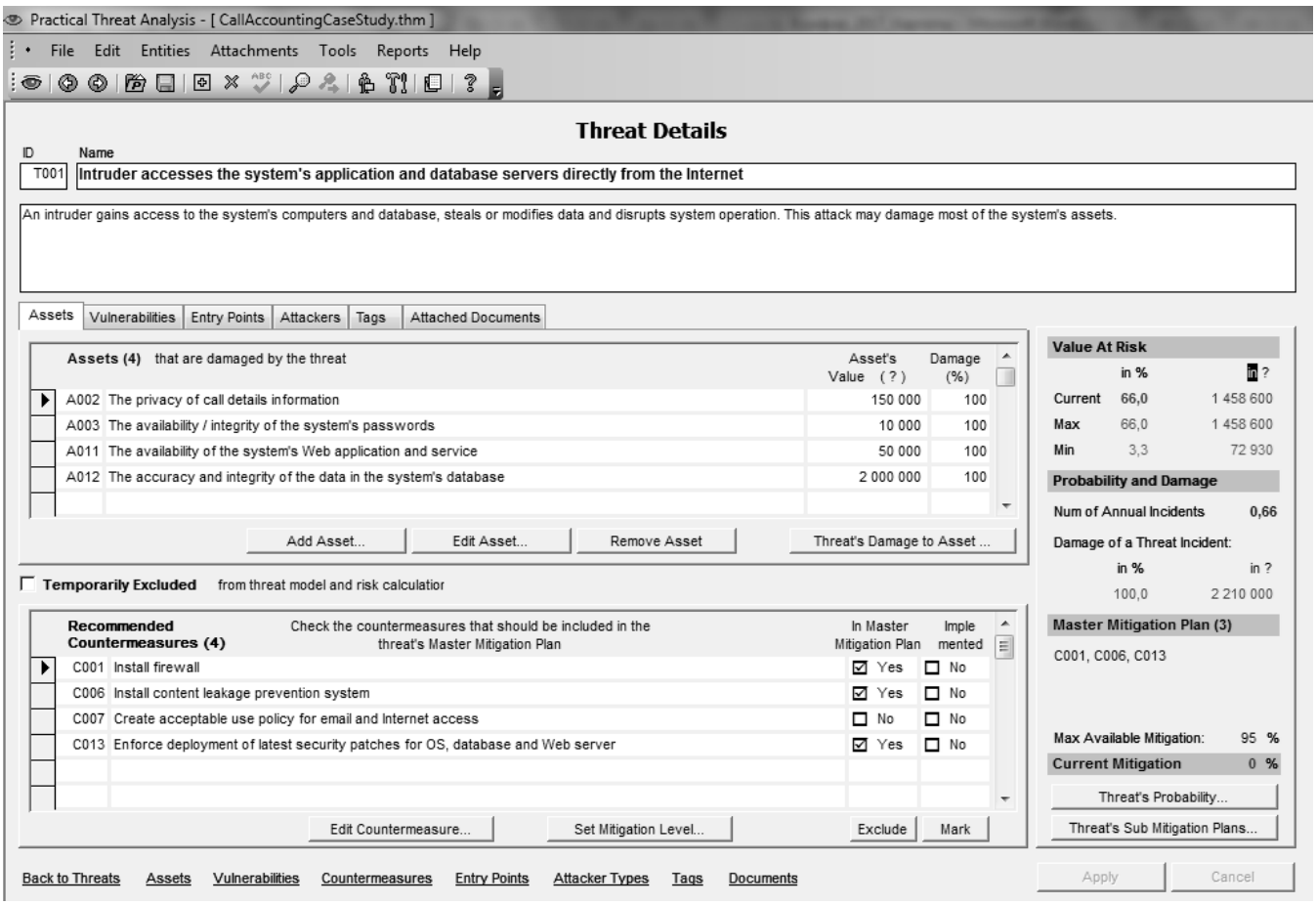

Рис. 7. Пример формы для фиксирования угроз и оценивания риска

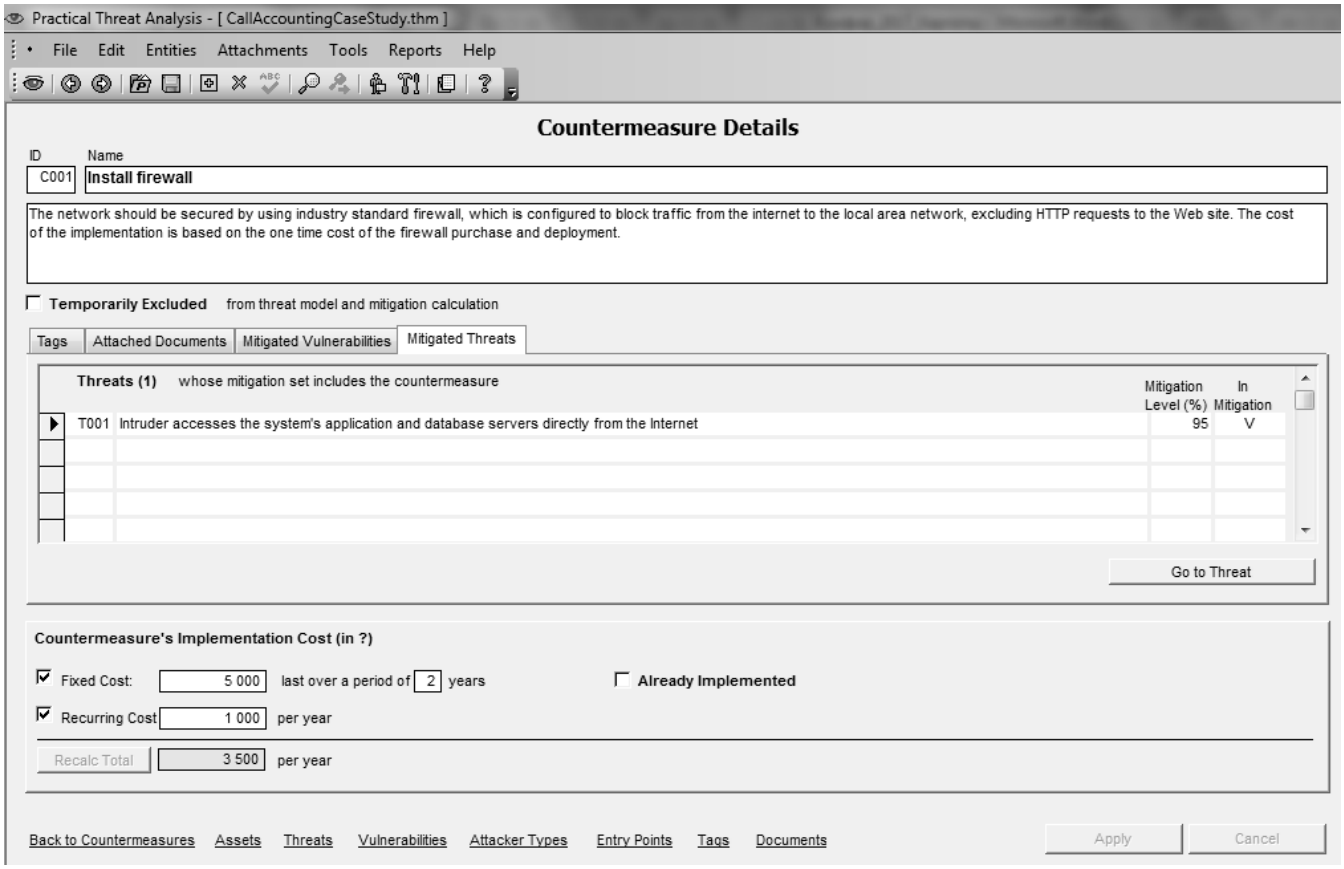

Рис. 8. Пример формы для фиксирования контрмер

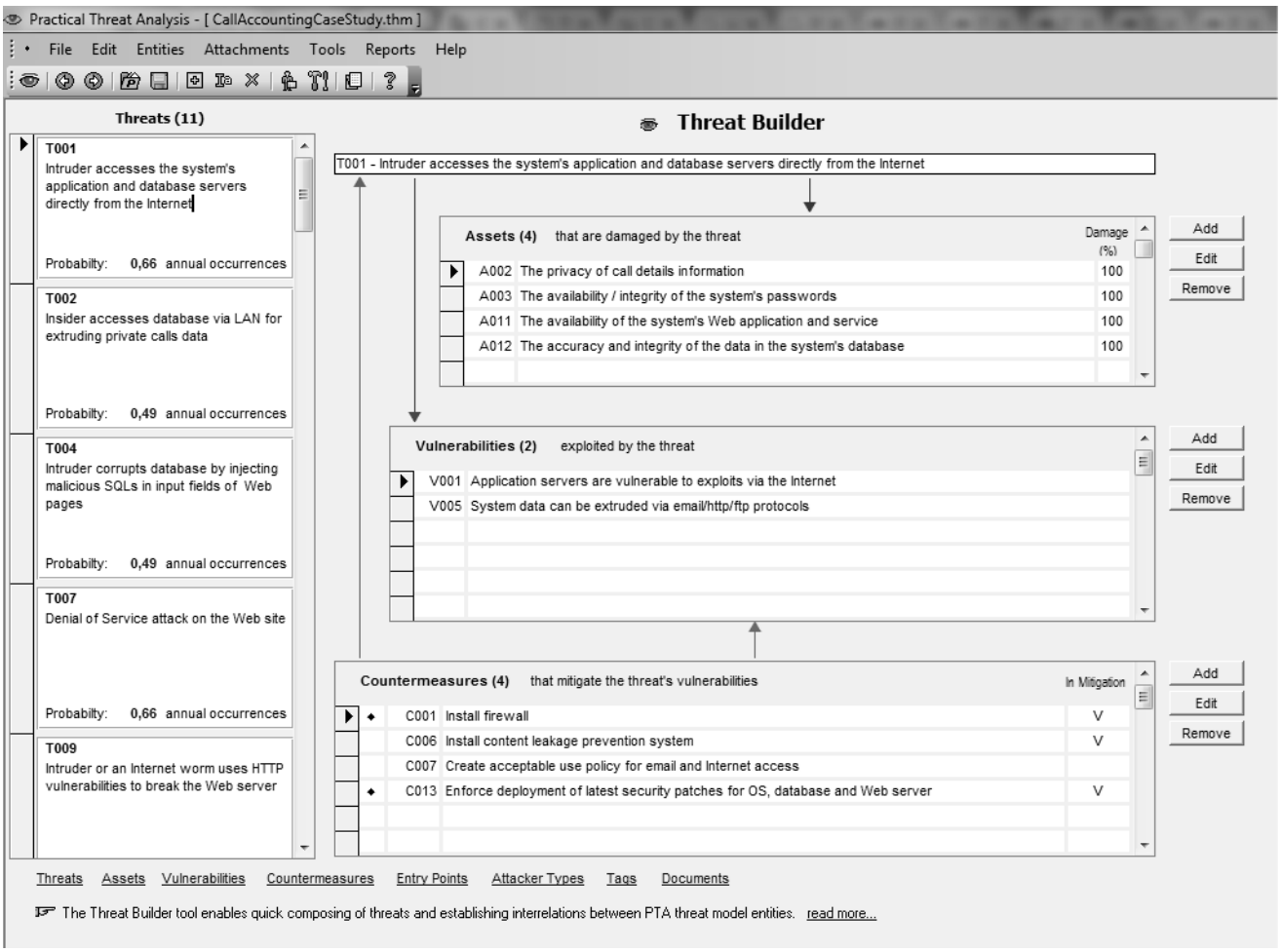

Рис. 9. Пример взаимосвязи РИС, уязвимости, угрозы и контрмер

Det-AOP и **Fuz-AOP** системы [7] соответственно основываются на детерминированном (DetM) (основанный на бинарных оценках) и нечетком (FuzM) методах оценивания. В системах ОР DetM и FuzM оценивания реализовывается посредством девяти шагов. Шаг 1 – определение множеств. Шаг 2 – описание оценочных компонент. Шаг 3 – оценка уровня значимости оценочных компонент. Шаг 4 – определение эталонных значений степени риска. Шаг 5 – определение эталонных значений оценочных компонент. Шаг 6 – оценка текущих значений компонент. Шаг 7 – классификация текущих значений. Шаг 8 – оценка степени риска. Шаг 9 – лингвистическое распознавание.

Непосредственно для ОР используются оценочные компоненты ***P, F, L*** и ***D.*** Так, для этих систем можно составить следующий кортеж ***<E, D, L, F, M, P, V(A)>***.

Все данные, полученные в процессе исследования представленных СОР, для удобства занесем в таблицу 9.

Таблица 9

Сведённые данные анализа СОР

АК / СОР	*AES*	*CA*	*CS*	*D*	*DT*	*E*	*F*	*L*	*M*	*P*	*SC*	*V(A)*	*VA*
Coras	–	–	±	±	–	±	–	–	±	+	–	+	–
Ebios	–	–	±	+	–	+	–	–	±	+	–	+	–
ISAMM	–	–	±	±	–	+	–	+	±	+	–	+	–
$IRAM_2$	–	–	±	±	–	±	–	–	±	+	–	+	–
PTA	–	–	±	±	–	±	–	+	±	+	–	+	–
Det-AOP	–	–	±	+	±	+	+	+	±	+	–	+	–
Fuz-AOP	–	–	±	+	±	+	+	+	±	+	–	+	–

Как видно из табл. 9, ни одно из анализируемых средств не обладает полным наборам характеристик риска из АК.

Таким образом, в работе с учетом предложенного в [1] подхода, проведено исследование СОР и определен набор базовых характеристик риска, которые представлены в виде кортежа для каждого из анализируемого средства. Как видно из сводной таблицы, для оценки во всех исследованных СОР используется вероятность ***P***, что в свою очередь подразумевает наличие определенной статистики об угрозах ИБ, которая собирается не во всех организациях. Также для работы с такими СОР существует необходимость в привлечении экспертов соответствующей предметной области.

ЛИТЕРАТУРА

[1]. Корченко А.Г. Бистабильная интегрированная кортежная модель характеристик риска / А.Г. Корченко, С.В. Казмирчук, А.Ю. Гололобов, Ю.А. Дрейс // Защита информации – 2016. – Том 18 №4. – С. 314-323.

[2]. Model-Driven Risk Analysis. Chapter: A Guided Tour of the CORAS Method, Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen, 2011, SINTEF ICT, Oslo, Norway, pp 23-43.

[3]. Expression des Besoins et Identification des Objectifs de Sécurité EBIOS, Méthode de gestion des risques, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

[4]. Quantitative Risk Assessment with ISAMM on ESA's Operations Data System [Electronic resource] [Carlo Harpes, André Adelsbach, Stefano Zatti, Nestor Peccia] / Itrust consulting, 2017 – Access mode: World Wide Web. – URL: https://www.itrust.lu/ wp-content/uploads/ 2007/ 09/publications_ TTC_ 2007_abstract_risk_assessment_with_ISAMM.pdf (19.01.2017).

[5]. IRAM$_2$ Managing information risk is a business essential [Electronic resource] / Information Security Forum Limited, 2014 – Access mode: World Wide Web. – URL: https://www.securityforum.org/ uploads/2015/03/ISF-IRAM2-ES.pdf (20.01.2017).

[6]. Practical Threat Analysis in-depth [Electronic resource] / PTA Technologies, 2013 – Access mode: World Wide Web. – URL: http://www.ptatechnologies.com/default.htm (20.01.2017).

[7]. Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук // Монография. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

[8]. Шевченко А. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційно-телекомунікаційних систем під час інформаційних операцій / А. Шевченко, О. Кокотов // Безпека информации – 2014. – Том 20 №1. – С. 7-11.

REFERENCES

[1]. Korchenko A., Kazmirchuk S., Gololobov A., Dreis Yu. Bistable and integrated based tuple model of risk characteristics, Zahist ìnformacìï, 2016, №4, pp. 314-323.

[2]. Model-Driven Risk Analysis. Chapter: A Guided Tour of the CORAS Method, Mass Soldal Lund, Bjørnar Solhaug, Ketil Stølen, 2011, SINTEF ICT, Oslo, Norway, pp 23-43.

[3]. Expression des Besoins et Identification des Objectifs de Sécurité EBIOS, Méthode de gestion des risques, ANSSI/ACE/BAC, Paris, Version du 25 janvier 2010, 95 p.

[4]. Quantitative Risk Assessment with ISAMM on ESA's Operations Data System [Electronic resource] [Carlo Harpes, André Adelsbach, Stefano Zatti, Nestor Peccia] / Itrust consulting, 2017 – Access mode: World Wide Web. – URL: https://www.itrust.lu/ wp-content/uploads/ 2007/ 09/publications_ TTC_ 2007_abstract_risk_assessment_with_ISAMM.pdf (19.01.2017).

[5]. IRAM2 Managing information risk is a business essential [Electronic resource] / Information Security Forum Limited, 2014 – Access mode: World Wide Web. – URL: https://www.securityforum.org/ uploads/2015/03/ISF-IRAM2-ES.pdf (20.01.2017).

[6]. Practical Threat Analysis in-depth [Electronic resource] / PTA Technologies, 2013 – Access mode: World Wide Web. – URL: http://www.ptatechnologies.com/default.htm (20.01.2017).

[7]. Korchenko A.G., Kazmirchuk S.V., Arkhipov A.E. The analysis and assessment risks information security. Monograph, 2013, 275 p.

[8]. Shevchenko A., Kokotov O. Method of risk assessment considering the security mechanism influence on parameters of the wireless information & telecommunication systems in the information operations, Bezpeka ìnformacìï, 2014, №1, pp. 7-11.

ДОСЛІДЖЕННЯ ЗАСОБІВ ОЦІНЮВАННЯ РИЗИКІВ БЕЗПЕКИ РЕСУРСІВ ІНФОРМАЦІЙНИХ СИСТЕМ

Одним з основних етапів побудови комплексних систем забезпечення безпеки ресурсів інформаційних систем є оцінювання ризиків. Часто перед фахівцями компаній для підвищення ефективності вирішення завдань захисту інформації виникає питання про вибір адекватного засобу оцінювання ризиків інформаційної безпеки, який буде задовольняти відповідні вимоги. На сьогодні існує досить широка множина таких засобів. Для їх раціонального вибору проведено дослідження множини засобів оцінювання ризиків з метою визначення набору необхідних порівняльних характеристик. Щодо зазначених засобів з урахуванням відомої аналітико-синтетичної кортежної моделі характеристик ризику формується кортеж, який дає можливість щодо певних параметрів уніфікувати процес порівняльного аналізу таких засобів. Це підвищить ефективність здій-

снення їх вибору для вирішення відповідних завдань інформаційної безпеки.
Ключові слова: інформаційна безпека, ризик, оцінювання ризиків, аналітико-синтетична кортежна модель, засоби оцінювання ризиків інформаційної безпеки, загроза, вразливість, характеристики ризику.

RESEARCH BASED ON TOOLS INVESTIGATION OF SECURITY RISK ASSESSMENT ACCORDING TO THE INFORMATION SYSTEMS RESOURCES

One of the main stages of integrated systems construction for protecting information resources is risk assessment. Often, specialists of the companies to increase the efficiency of information security pay attention to the choice of adequate tools of information security risks assessment that will meet the relevant requirements. Nowadays there is a wide range of such tools. For their rational choice, a variety of risk assessment tools have been investigated to determine the set of necessary comparative characteristics. According to the mentioned means, taking into account the known analytical-synthetic tuple model of risk characteristics, a tuple is formed, which makes it possible due to the certain parameters, to unify the process of comparative analysis of such means. This will enhance the effectiveness of the choice implementation to solve the corresponding tasks of information security.
Keywords: information security, risk, risk assessment, analytic-synthetic tuple model, tools for information security risk assessment, threat, vulnerability, risk characteristics.

Приставка Филипп Александрович, доктор технических наук, профессор, заведующий кафедрой прикладной математики Национального авиационного университета.
E-mail: chindakor@mail.ru

Приставка Пилип Олександрович, доктор технічних наук, професор, завідувач кафедри прикладної математики Національного авіаційного університету.
Prystavka Philip, Dr Eng, professor, head of applied mathematics department, National Aviation University.

Павленко Петр Николаевич, доктор технических наук, профессор, профессор кафедры средств защиты информации Национального авиационного университета.
E-mail: petrpav@nau.edu.ua
Павленко Петро Миколайович, доктор технічних наук, професор, професор кафедри засобів захисту інформації Національного авіаційного університету.
Pavlenko Petro, Dr Eng, professor, professor of information security means department, National Aviation University.

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.

Коломиец Марина Вячеславовна, студентка Национального авиационного университета.
E-mail: mk160597@mail.ru
Коломієць Марина В'ячеславівна, студентка Національного авіаційного університету.
Kolomiiets Maryna, student, National Aviation University..

DOI: 10.18372/2410-7840.19.11444
УДК 004.056.5

ЗАХИСТ ОПЕРАЦІЙНОГО СЕРЕДОВИЩА СИСТЕМ ІНТЕРНЕТ ГОЛОСУВАННЯ

Володимир Чуприн, Володимир Вишняков, Михайло Пригара

В даній роботі запропоновано метод створення захищеного операційного середовища для сервера системи Інтернет голосування, який усуває причини недовіри суспільства щодо можливих фальсифікацій результатів або розкриття таємниці голосів. Метод базується на концепції ядра безпеки і реалізує профіль захищеності, згідно якому в оперативній пам'яті сервера створюється ділянка, в межах якої доступ до даних має виключно процес підрахунку голосів наперед вибраною відкритою прикладною програмою. Для унеможливлення доступу до цієї ділянки пам'яті для будь-яких інших процесів, використано відкриту операційну систему, у якій функції для такого доступу відсутні. Крім того, створено умови для дистанційного контролю цілісності усіх без винятку файлів і процесів на сервері, а також всіх дій персоналу щодо адміністрування сервера з боку необмеженої кількості контролерів, якими можуть стати будь-які особи. Показано, що запропонований метод в сукупності з відомими методами захисту інформації, надає змогу виявлення всіх можливих