НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №1, 2011

УДК 004.056.5(045) **Корченко А.Г., Иванченко Е.В.**, **Казмирчук С.В. (НАУ)**

ИНТЕГРИРОВАННОЕ ПРЕДСТАВЛЕНИЕ ПАРАМЕТРОВ РИСКА

Был проведен анализ понятия риска в различных предметных областях с точки зрения безопасности, психологии, экономики, страхования, медицины, геологии и т.д., которое раскрывалось как в монографиях, статьях, учебниках, словарях так и в различных нормативных национальных и международных документах. Определены базовые характеристики риска из множества его толкований для последующей интерпретации в информационной безопасности. Предлагается для интеграции определения понятия риска, с отображением в области ИБ, представить его в виде кортежа с описанием идентифицирующих и несущих компонентов.

Ключевые слова: информационная безопасность, риск, степень риска, кортеж.

В работе [3] проведен анализ толкований риска во многих отраслях человеческой деятельности с целью его отображения на сферу информационной безопасности (ИБ), а также выделены базовые характеристики риска, которые можно интерпретировать, как его параметры.

Существующие методики оценки и анализа риска ИБ за основу берут только несколько параметров, например, вероятность, опасность и частоту. Часто при построении систем менеджмента ИБ или при проведении ее аудита, возникают случаи, при которых необходимо отразить риск через другие параметры, например, таких как, затраты и потери, неопределённость, характеристика ситуации и т.д. В этой связи целью данной работы является анализ параметров риска, определение их свойств и допустимых вариантов формирования возможных взаимосвязей между ними.

Для исследуемого множества толкований риска, в работе [3], выделены его базовые признаки: риск рассматривается как измеряемая или рассчитываемая вероятность; риск связан с наступлением определенного события (как правило, не благоприятного); понятие риска раскрывается через деятельность субъекта; риск раскрывается через независящее от деятельности субъекта событие; понятие риска рассматривается, как мера, акцент делается на количественную и качественную оценку риска – “меру риска”; понятие риска раскрывается через неопределенность; риск отображается ситуацией выбора из двух или из *n* вариантов действия; риск воспринимается как опасность, частота, затраты и потери, характеристика ситуации, суммарная величина, а также с учетом [5] риск можно трактовать, как отклонение от цели.

Предлагается для интегрированного представления параметров риска с отображением на сферу ИБ, представить его в виде десятикомпонентного кортежа **<E, A, M, C, P, D, S, F, L, V>,** где **E** – событие, **A** – действие, **M** – мера риска, **C** – характеристика ситуации, **P** – вероятность, **D** – опасность, **S** – ситуация выбора, **F** – частота, **L** – затраты и потери (расходы), **V** – отклонение от цели.

Первый приведённый в кортеже компонент – **событие (E),** который можно отображать в виде символьной переменной, принимающей одно из значений конечного множества идентификаторов $E \in \{E_1, E_2, ..., E_e\}$ (*e* – количество идентификаторов событий). С учетом того, что в области ИБ риск связан с такими базовыми характеристиками безопасности ресурсов информационных систем (РИС) как конфиденциальность, целостность и доступность, то базовые события при *e*=7 могут идентифицироваться как, E_1=“Нарушение конфиденциальности (НК)”, E_2=“Нарушение целостности (НЦ)”, E_3=“Нарушение доступности (НД)”, E_4=“Нарушение целостности и конфиденциальности (НЦК)” E_5=“Нарушение целостности и доступности (НЦД)” E_6=“Нарушение конфиденциальности и доступности (НКД)” E_7=“Нарушение конфиденциальности, целостности и доступности (НКЦД)”.

Следующий компонент кортежа – **действие (A),** которое привело к событию **E**. С точки зрения ИБ **A** связано с реализацией потенциальных **угроз** базовым характеристикам

безопасности РИС, которые привели к возникновению **E,** отображаемого одним из идентификаторов $\{E_1, E_2, ..., E_7\}$. В связи с этим, по аналогии с **E,** компонент **A** можно отобразить множеством идентификаторов $A \in \{A_1, A_2, ..., A_a\}$ (где a – количество идентификаторов угроз), например, A_1="Компьютерный шпионаж", A_2="Шпионаж", A_3="Сбой программного обеспечения" и т.д.

Прежде чем раскрыть компонент **меру риска (M)**, отметим, что одной из базовых процедур, производимых над риском, является его измерение (оценка) [2]. В [6], по способу получения значения измеряемой величины, определенны (как основные) прямые и косвенные измерения. При прямом измерении, искомое значение величины находят непосредственно из опытных данных (т.е. измеряемая величина непосредственно сравнивается с мерой), а при косвенном – на основании известной зависимости этой величины и величин, получаемых прямыми измерениями.

В ряде случаев, когда нет прямых шкал, используют либо прямые шкалы других свойств (связанных с интересующими нас) либо определяют новые [8]. Примером является шкала для измерения субъективного свойства "ценность информационного ресурса". Она может измеряться в производных шкалах, например, таких как стоимость или время восстановления ресурса и др. Альтернативный вариант – определить шкалу для получения экспертной оценки, например, имеющую три значения: малоценный информационный ресурс (от него не зависят критически важные задачи и его восстановление связано с небольшими затратами времени и денег); ресурс средней ценности (от него зависит ряд важных задач, но в случае его утраты возможно восстановление за некритически допустимое время, а стоимость восстановления высокая); ценный ресурс (от него зависят критически важные задачи и в случае его утраты время восстановления превышает критически допустимое, либо стоимость чрезвычайно высока). Для измерения рисков пока не существует естественной – простой шкалы и поэтому их оценивают по объективным либо субъективным критериям [8]. Примером объективного критерия является вероятность выхода из строя какого-либо оборудования, например, ПК за определенный промежуток времени, а субъективного – оценка (владельцем информационного ресурса) риска выхода из строя ПК. Для этого обычно разрабатывается качественная шкала с несколькими градациями, например: низкий, средний и высокий уровни [8].

Для измерения риска в сфере ИБ обычно используются качественные и количественные шкалы: вероятностные, денежные [7], лингвистические [1], бинарные [1, 9], а также возможны измерения с помощью коэффициентов. В этой связи, компонент **M,** с учетом характера измерений в области ИБ, можно отобразить трехкомпонентным множеством $M \in \{M_{кл}, M_{кч}, M_{и}\}$, где $M_{кл}$ – количественная (например, характеризуемая численно), $M_{кч}$ – качественная (например, характеризуемая лингвистически) и $M_{и}$ – интегрированная (например, характеризуемая численно и лингвистически) меры.

В работе [3] понятие риска, во множестве его толкований, раскрывается так же через неопределённость. С точки зрения ИБ базовый признак риска **неопределённость** можно интерпретировать, как **характеристику ситуации** при наступлении определённого события **E.** В ИБ может наступить событие **E,** к которому привело действие **A,** которое ранее не происходило, например, нет статистических данных о конкретном виде инцидента нарушения ИБ. Следовательно, рассматривая компонент кортежа **характеристика ситуации (C),** можно отобразить его двухкомпонентным множеством $C \in \{C_o, C_н\}$ где, C_o – характеризирует ситуацию как определённую, а $C_н$ – как нечеткую.

Четвертый компонент кортежа **вероятность (P)** появления события **E (**например, с идентификатором E_3). Вероятность часто разделяют на "объективную" (иногда называемую физической) и "субъективную" [10]. Под объективной вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или

отношение числа благоприятных исходов к их общему количеству. Она, например, формируется при анализе результатов большого числа наблюдений. Под субъективной вероятностью понимается мера уверенности некоторого человека или группы людей в том, что данное событие произойдет. Эта вероятность может быть формально представлена различными способами, например, вероятностным распределением или бинарным отношением на множестве событий, но наиболее часто она представляет собой вероятностную меру, полученную экспертным путем [10]. Следует отметить, что когда возникают сложности с получением статистических данных, а так же для простоты интерпретации величин, эксперты используя логико-лингвистический подход отображают этот компонент через лингвистическую переменную (ЛП) [4] “ВЕРОЯТНОСТЬ” с базовым терм-множеством $\mathbf{P} = \mathop{\text{Y}}_{i=1}^{p} \text{P}_i$ (p – количество термов), для членов которого справедливо отношение порядка $\text{P}_1 < \text{P}_2 < ... < \text{P}_p$. Например, при p=3 для указанной ЛП можно сформировать множество термов $\mathbf{P} = \mathop{\text{Y}}_{i=1}^{3} \text{P}_i =$ {“низкая (Н)”, “средняя (С)”, “высокая (В)”}, отображаемых нечеткими числами $\underset{\sim}{\text{Н}}, \underset{\sim}{\text{С}}, \underset{\sim}{\text{В}}$, для которых (используя известные методы [4]) определяются соответствующие функции принадлежности. Также могут быть введены и другие значения первичных термов такие как, например, “очень низкая (ОН)”, “выше среднего (ВС)”, “ниже среднего (НС)” и др. Очевидно, что в этом случае **P** отображается в лингвистической форме и при этом логически следует, что **M** интерпретируется, как $\text{M}_{кч}$.

Компонент **ситуация выбора (S)** в области ИБ можно интерпретировать как величину, характеризирующую предпочтительность наступления состояния **E.** На основе этого компонента удобно принимать решения по организации мероприятий, например, по снижению риска, его принятию, передачи третьему лицу и т.д. Компонент **S**, аналогично **вероятности,** можем представить через ЛП “СИТУАЦИЯ ВЫБОРА” с базовым терм-множеством $\mathbf{S} = \mathop{\text{Y}}_{i=1}^{s} \text{S}_i$ ($\text{S}_1 < \text{S}_2 < ... < \text{S}_s$), позволяющего интерпретировать выбор посредством s вариантов. Например, при s=2 для указанной ЛП может быть сформировано $\mathbf{S} = \mathop{\text{Y}}_{i=1}^{2} S_i =$ {“менее привлекательная (МП)”, “более привлекательная (БП)”} или $\mathbf{S} = \mathop{\text{Y}}_{i=1}^{2} S_i =$ {“менее надежная (МН)”, “более надежная (БН)”}, которые соответственно отображаются нечеткими числами $\underset{\sim}{\text{МП}}, \underset{\sim}{\text{БП}}$ или $\underset{\sim}{\text{МН}}, \underset{\sim}{\text{БН}}$ [3, 4].

Компонент кортежа **опасность (D)** рассматривается как величина характеризующая опасность события, например, E_1 посредством A_2). По аналогии с **P** компонент **D** может отображаться численно (например, в процентах) или с помощью ЛП – “ОПАСНОСТЬ” с базовым терм-множеством $\mathbf{D} = \mathop{\text{Y}}_{i=1}^{d} \text{D}_i$ ($\text{D}_1 < \text{D}_2 < ... < \text{D}_d$). Например, при d=3 можем определить $\mathbf{D} = \mathop{\text{Y}}_{i=1}^{3} \text{D}_i =$ {“низкая (Н)”, “средняя (С)”, “высокая (В)”}, а **мере** будет соответствовать $\text{M}_{кч}$.

Следующий компонент кортежа **частота (F),** который в области ИБ можно связать с частотой реализации “угрозы”, приведшей к событию **E**. Такой компонент можно

отображать численно или через ЛП – “ЧАСТОТА”: $\mathbf{F} = \mathop{Y}_{i=1}^{f} F_i$ ($F_1 < F_2 < ... < F_f$), например, при f=3 – $\mathbf{F} = \mathop{Y}_{i=1}^{3} F_i$ = {“низкая (Н)”, “средняя (С)”, “высокая (В)”}.

Компонент **затраты и потери** в области ИБ целесообразно определить через термин **расходы (L),** который по аналогии с предыдущим можно представлять числено, например, 1) 0 - $100; 2) $100 - $1000; 3) $1000 - $10 000; 4) $10 000 - $100 000, при этом **мере** соответствует $М_{кл.}$ Также **L** можно представить с помощью ЛП “РАСХОДЫ”: – $\mathbf{L} = \mathop{Y}_{i=1}^{l} L_i$ ($L_1 < L_2 < ... < L_l$), например, при l=5 – $\mathbf{L} = \mathop{Y}_{i=1}^{5} L_i$ = {“низкие (Н)”, “ниже среднего (НС)”, “средние (С)”, “выше среднего (ВС)”, “высокие (В)”}, а **M** соответствует $М_{кч}$. На практике встречается и интегрированное представление **L,** например, 1) *Negligible* (менее $100); 2) *Minor* (менее $1000); 3) *Moderate* (менее $10 000); 4) *Serious* (Существенное негативное влияние на бизнес); 5) *Critical* (Катастрофическое воздействие, возможно прекращение деятельности предприятия) [11], при этом **мера** будет отображаться параметром $М_{и}$**.**

Отклонение от цели (нормы) (V) – этот компонент, как и **P** может отображаться числено (например, как стандартное (квадратичное), вероятное или допускаемое отклонение [12]), так и посредством применения логико-лингвистического подхода с помощью ЛП “ОТКЛОНЕНИЕ ОТ ЦЕЛИ”: $\mathbf{V} = \mathop{Y}_{i=1}^{v} V_i$ ($V_1 < V_2 < ... < V_v$). Например, при v=3 можно сформировать множество термов $\mathbf{V} = \mathop{Y}_{i=1}^{3} V_i$ = {“маленькое (М)”, “среднее (С)”, “большое (Б)”}, отображаемых нечеткими числами $\underset{\sim}{М}, \underset{\sim}{С}, \underset{\sim}{Б}$.

Следует отметить, что при представлении риска, с помощью кортежа, можно выделить его идентифицирующие **E, A, M, C** и оценочные компоненты **P**, **D**, **S**, **F**, **L** и **V**.

Идентифицирующие компоненты выступают в качестве интегрированного идентификатора риска и могут, отображаются с помощью оценочных компонент посредством числовых или лингвистических значений (показателей), например, для информационной системы компании необходимо определить риск, связанный с наступлением события нарушения ИБ, которое привело к воздействию на целостность и доступность – это событие идентифицируется как $Е_5$=“НЦД”, а действие, которое привело к нему, например, $А_3$=“Сбой программного обеспечения”. Здесь для отображения риска можем использовать $М_{кл}$, $М_{кч}$ или $М_{и}$, а для того чтобы показать его значащие параметры следует воспользоваться оценочными компонентами кортежа, а именно, например, определить: вероятность (**P)** наступления такого события, к которому привело это действие; опасность (**D)** от наступления события; расходы (**L),** которые будут результатом наступления события; частоту (**F)** наступления данного события (действия); отклонения от цели (**V)** и наконец, выбрать вариант принятия решений **(S)**.

Для приведенных оценочных компонентов кортежа, могут быть определены зависимости (например, аналитические) или корреляции (например, на уровне системы лингвистического вывода). Рассмотрим пример с параметрами **P, D, F** и **L,** показывающий взаимосвязь (на уровне лингвистического вывода) оценочных компонентов **D, P** и **F,** посредством зависимости параметров для **D** и **L,** заданных в табл. 1 и табл. 2.

Зависимость параметров **P** и **F** для **D** Таблица 1

Вероятность (**P**)	Частота (**F**)

	“Высокая (В)”	“Средняя (С)”	“Низкая (Н)”
“Высокая (В)”	“В”	“С”	“Н”
“Средняя (С)”	“С”	“С”	“Н”
“Низкая (Н)”	“Н”	“Н”	“Н”

Пусть по отношению к информационной системе произошло действие A_3= “Сбой программного обеспечения” и определены (для **D**) соответствующие зависимости параметров **P** и **F** (см. табл. 1). Тогда на основе этих зависимостей можно отобразить **D** посредством следующих правил:

1) ЕСЛИ Вероятность (**P**) A_3 “Высокая” И Частота (**F**) реализации такого A_3 “Высокая” ТОГДА Опасность (**D**) при A_3 для информационной системы = Высокая;
2) ЕСЛИ P (A_3) “В” И F (A_3) “С” ТОГДА D (A_3) = “С”;
3) ЕСЛИ P (A_3) “В” И F (A_3) “Н” ТОГДА D (A_3) = “Н”;
4) ЕСЛИ P (A_3) “С” И F (A_3) “В” ТОГДА D (A_3) = “С”;
5) ЕСЛИ P (A_3) “С” И F (A_3) “С” ТОГДА D (A_3) = “С”;
6) ЕСЛИ P (A_3) “С” И F (A_3) “Н” ТОГДА D (A_3) = “Н”;
7) ЕСЛИ P (A_3) “Н” И F (A_3) “В” ТОГДА D (A_3) = “Н”;
8) ЕСЛИ P (A_3) “Н” И F (A_3) “С” ТОГДА D (A_3) = “Н”;
9) ЕСЛИ P (A_3) “Н” И F (A_3) “Н” ТОГДА D (A_3) = “Н”.

Аналогично можем определить зависимости (см. табл. 2) и построить возможные взаимосвязи для компонентов **D, F** и **L**.

Зависимость параметров **D** и **F** для **L** Таблица 2

Опасность (**D**)	Частота (**F**)		
	“Высокая (В)”	“Средняя (С)”	“Низкая (Н)”
“Высокая (В)”	“В”	“ВС”	“НС”
“Средняя (С)”	“ВС”	“С”	“НС”
“Низкая (Н)”	“НС”	“НС”	“Н”

1) ЕСЛИ Опасность (**D**) A_3 “Высокая” И Частота (**F**) A_3 “Высокая” ТОГДА Расходы (**L**) A_3 = Высокие (В);
2) ЕСЛИ D (A_3) “В” И F (A_3) “С” ТОГДА L (A_3) = “ВС”;
3) ЕСЛИ D (A_3) “В” И F (A_3) “Н” ТОГДА L (A_3) = “НС”;
4) ЕСЛИ D (A_3) “С” И F (A_3) “В” ТОГДА L (A_3) = “ВС”;
5) ЕСЛИ D (A_3) “С” И F (A_3) “С” ТОГДА L (A_3) = “С”;
6) ЕСЛИ D (A_3) “С” И F (A_3) “Н” ТОГДА L (A_3) = “НС”;
7) ЕСЛИ D (A_3) “Н” И F (A_3) “В” ТОГДА L (A_3) = “НС”;
8) ЕСЛИ D (A_3) “Н” И F (A_3) “С” ТОГДА L (A_3) = “НС”;
9) ЕСЛИ D (A_3) “Н” И F (A_3) “Н” ТОГДА L (A_3) = “Н”.

Следует отметить, что многие известные методики для управления, анализа и оценки риска в сфере ИБ, (например, Cobra, NIST 800-30, CRAMM и т. д.) используют в качестве исходящих параметров **P** и **L,** но как видно из [3] часто требуются альтернативные варианты. Если необходимо отобразить риск через другие параметры, то нужно расширить известные методики за счет дополнительных модулей, устанавливающих соответствующие взаимосвязи между заданными величинами (характеризующими риск) и искомыми. Это позволит повысить гибкость существующих методик оценки и анализа риска и расширит возможности их использования.

Литература

1. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology [Электронный ресурс] / NIST, Special Publication 800-30 – Режим доступа: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

2. Suominen, Mercurius. [Электронный ресурс] / Suominen, Arto. // Turku– 1994. – № 5. pp 14 –17. – Режим доступа: http://ieeexplore.ieee.org/iel3/4232/12270/00569765.pdf

3. Корченко А.Г. Анализ и определение понятия риска для его интерпретации в области информационной безопасности / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Научно-технический журнал "Защита информации" – 2010. – №3. – С. 5-10.

4. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А.Г. – К. : "МК-Пресс", 2006. – 320с. (ил. Монография).

5. К вопросу об определении понятия "риск" [Электронный ресурс] / В.В. Индеева // РГМУ им. акад. И.П. Павлова Рязань, Россия – Режим доступа к статье: http://www.rae.ru/zk/arj/2007/02/Indeeva.pdf

6. Любимов Л. И. Поверка средств электрических измерений: справ. книга / Любимов Л. И., Формсилова И. Д., Шапиро Е. З.. – Л.: Энергоатомиздат, 1987. – 296 с.

7. Монте-Карло для аналитиков. Как грамотно моделировать и измерять риски. [Электронный ресурс] / Андрей Лукашов // Риск-менеджмент. – 2007. – №3 – С. 73-77. – Режим доступа: http://www.ecsocman.edu.ru/images/pubs/2007/04/27/0000307302/72-77-praktikum_-_lukashev_SCR.pdf

8. Петренко С. А Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М.: Компания АйТи ; ДМК Пресс, 2004. – 384 с.: ил.

9. Руководство по управлению рисками безопасности. [Электронный ресурс] / Группа разработки решений Майкрософт по безопасности и соответствию, регулятивным нормам и Центр Microsoft security center of excellence. – Режим доступа: http://www.microsoft.com/rus/technet/security/guidance/complianceandpolicies/secrisk/

10. Симонов С. С. Технологии и инструментарий для управления рисками / Симонов С. С. // Информационный бюллетень Jet Info. – 2003. – № 2 (117)/2003. – С. 3 – 32.

11. Технологии анализа рисков. Окончание. [Электронный ресурс] / Компьюлинк – Режим доступа: http://pda.cio-world.ru

12. Широков К. П. "Большой советской энциклопедии" [Электронный ресурс] / "Советская энциклопедия" в 1969 — 1978 годах в 30 томах. – Режим доступа: http://slovari.yandex.ru

Надійшла: 19.03.11

Рецензент: д.т.н, проф. Хорошко В.О.