УДК 004.056.5(045)

С.В. Казмирчук, ассистент
(Национальный авиационный университет, Украина)

БАЗОВЫЕ ПАРАМЕТРЫ РИСКА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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.

В работе [1] 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 описанных параметров риска, определение их свойств и связей между ними.

Для исследуемого множества толкований риска (с отображением на сферу ИБ) в работе [1] выделены его базовые признаки, которые с учетом [3] (риск – как отклонение от цели), предлагается представить его в виде кортежа с десятью компонентами **< 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 е=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 $E \in \{E_1, E_2, ..., E_7\}$. 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.

Компонент **мера риска (M),** с учетом характера измерений в области ИБ, можно отобразить трехкомпонентным множеством $M \in \{M_{кл}, M_{кч}, M_u\}$, где $M_{кл}$ – количественная (например, характеризуемая численно), $M_{кч}$ – качественная (например, характеризуемая лин-

гвистически) и M_u – интегрированная (например, характеризуемая численно и лингвистически) меры.

В работе [1] 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 **Е.** В ИБ может наступить событие **Е** к которому привело действие **А** которое ранее не происходило, например, нет статистических данных о конкретном виде инцидента нарушения ИБ. Следовательно, рассматривая компонент кортежа **характеристика ситуации (С),** 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 (Р)** появления события **Е (**например, с идентификатором E_3). Её часто разделяют на "объективную" (иногда называемую физической) и "субъективную" [4]. Под объективной вероятностью понимается относительная частота появления какого-либо события в общем объеме наблюдений или отношение числа благоприятных исходов к их общему количеству. Эта вероятность, например, возникает 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 [4]. 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) [2] "ВЕРОЯТНОСТЬ" с базовым терм-множеством $\mathbf{P} = \bigcup_{i=1}^{p} P_i$ (p – количество термов), для членов которого справедливо отношение порядка $P_1 < P_2 < ... < P_p$. Например, при p=3 для указанной ЛП можно сформировать множество термов $\mathbf{P} = \bigcup_{i=1}^{3} P_i =$ {"низкая" (Н), "средняя" (С), "высокая" (В)}, отображаемых нечеткими числами $\underset{\sim}{Н}, \underset{\sim}{С}, \underset{\sim}{В}$, для которых (используя известные методы [2]) 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 **Р** отображается лингвистически и при этом логически следует, что **М** интерпретируется, как $M_{кч}$.

Компонент **ситуация выбора (S)** в области ИБ можно интерпретировать как величину, характеризирующую предпочтительность наступления состояния **Е.** 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 $\mathbf{S} = \bigcup_{i=1}^{s} S_i$ ($S_1 < S_2 < ... < S_s$) позволяющего интерпретировать выбор посредством s вариантов. Например, при s=2 для указанной ЛП может быть сформировано $\mathbf{S} = \bigcup_{i=1}^{2} S_i =$ {"менее привлекательная" (МП), "более привлекательная" (БП)} или $\mathbf{S} = \bigcup_{i=1}^{2} S_i =$ {"менее надежная" (МН), "более надежная" (БН)}, которые соответственно отображаются нечеткими числами $\underset{\sim}{МП}, \underset{\sim}{БП}$ или $\underset{\sim}{МН}, \underset{\sim}{БН}$ [1, 2].

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 $\mathbf{D} = \bigcup_{i=1}^{d} D_i$ $(D_1 < D_2 < ... < D_d)$. Например, при d=3 можем определить $\mathbf{D} = \bigcup_{i=1}^{3} D_i$ = {"низкая" (Н), "средняя" (С), "высокая" (В)}, а **мере** будет соответствовать $M_{кч}$.

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": $\mathbf{F} = \bigcup_{i=1}^{f} F_i$ $(F_1 < F_2 < ... < F_f)$, например, при f=3 – $\mathbf{F} = \bigcup_{i=1}^{3} F_i$ = {"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 $M_{кл.}$ Также **L** можно представить с помощью ЛП "РАСХОДЫ": – $\mathbf{L} = \bigcup_{i=1}^{l} L_i$ $(L_1 < L_2 < ... < L_l)$, например, при l=5 – $\mathbf{L} = \bigcup_{i=1}^{5} L_i$ = {"низкие" (Н), "ниже среднего" (НС), "средние" (С), "выше среднего" (ВС), "высокие" (В)}, а **M** соответствует $M_{кч}$. 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) [5], при этом **мера** будет отображаться параметром $M_{и}$**.**

Отклонение от цели (нормы) (V) – этот компонент, как и **P** может отображаться числено (например, как стандартное (квадратичное), вероятное или допускаемое отклонение [6]), так и посредством применения логико-лингвистического подхода с помощью ЛП "ОТКЛОНЕНИЕ ОТ ЦЕЛИ": $\mathbf{V} = \bigcup_{i=1}^{v} V_i$ $(V_1 < V_2 < ... < V_v)$. Например, при v=3 можно сформировать множество термов $\mathbf{V} = \bigcup_{i=1}^{3} V_i$ = {"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 отображаются с помощью оценочных компонент, например, для информационной системы компании необходимо определить риск связанный с наступлением события нарушения ИБ, которое привело к нарушению целостности и доступности – это событие идентифицируется как E_5= НЦД, к этому событию привело действие A_3="Сбой программного обеспечения", для отображения риска можем использовать $M_{кл}$, $M_{кч}$ так и $M_{и}$, для того чтобы показать величину риска можем воспользоваться оценочными компонентами кортежа, а именно 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 **S** принятия решений.

Для приведенных оценочных компонент кортежа, могут быть определены зависимости (например, аналитические) или корреляции (например, на уровне системы лингвистического вывода). Для примера рассмотрим следующие компоненты: P, S, D, F и L.

Рассмотрим пример связывающий оценочные компоненты **D, P** и **F,** соответственно с табл. 1 и 2 определяющей зависимости параметров для компонент **D** и **L**.

Таблица 1. Зависимости параметров для D

Вероятность (P)	Частота (F)		
	Высокая	Средняя	Низкая
Высокая	В	С	Н
Средняя	С	С	Н
Низкая	Н	Н	Н

Таблица 2. Зависимости параметров для L

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

Пусть произошло действие A_3= “Сбой программного обеспечения” и определены компоненты P и F (Табл. 1), тогда через эти компоненты можно отобразить D. Это можно записать следующими закономерностями: 1) ЕСЛИ Вероятность A_3 (P) “Высокая” И Частота реализации такого A_3 (F) “Высокая” ТОГДА Опасность наступления A_3 для информационной системы (D) = Высокая; 2) ЕСЛИ P “В” И F “С” ТОГДА D = С; 3) ЕСЛИ P “В” И F “Н” ТОГДА D = Н; 4) ЕСЛИ P “С” И F “В” ТОГДА D = С; 5) ЕСЛИ P “С” И F “С” ТОГДА D = С; 6) ЕСЛИ P “С” И F “Н” ТОГДА D = Н; 7) ЕСЛИ P “Н” И F “В” ТОГДА D = Н; 8) ЕСЛИ P “Н” И F “С” ТОГДА D = Н; 9)ЕСЛИ P “Н” И F “Н” ТОГДА D = Н.

Аналогично можем определить закономерности между компонентами D и F для L (Табл. 2): 1) ЕСЛИ Опасность (D) “Высокая” И Частота (F) “Высокая” ТОГДА Расходы (L) = Высокие (В); 2) ЕСЛИ D “В” И F “С” ТОГДА L = ВС; 3) ЕСЛИ D “В” И F “Н” ТОГДА L = НС; 4) ЕСЛИ D “С” И F “В” ТОГДА L =ВС; 5) ЕСЛИ D “С” И F “С” ТОГДА L = С и т.д.

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 вероятность и потери, для отображения риска в других параметрах необходимо подключение дополнительного модуля, который будет посредством установленных взаимосвязей определять риск через другие параметры.

Выводы. Интегрированное представление параметров риска (с отображением на сферу ИБ) в виде кортежа с определением идентифицирующих и несущих компонент, позволит сформировать взаимосвязи между отдельными параметрами. Это даст возможность более гибко и эффективно использовать для оценивания риска существующие методы и средства.

Список литературы

1. 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” №3, 2010 С. 5-10.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: “МК-Пресс”, 2006. – 320с., ил.

3. 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

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

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

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