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

АНАЛИЗ И ОПРЕДЕЛЕНИЕ ПОНЯТИЯ РИСКА ДЛЯ ЕГО ИНТЕРПРЕТАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Стремительное развитие IT-инфраструктуры предприятий неизменно влечет за собой неконтролируемый рост количества информационных угроз и уязвимостей информационных ресурсов. В этих условиях оценка информационных рисков позволяет определить необходимый уровень защиты информации, осуществить его поддержку и разработать стратегию развития информационной структуры компании. Оценка и анализ информационных рисков является необходимым условием при создании системы управления рисками и плана обеспечения непрерывности и возобновления бизнеса.

На сегодняшний день существует множество инструментальных средств, которые объединяются в методики оценки и анализа риска. Эти методики представляются в достаточно широком спектре, начинающегося нормативными документами (стандартами) и заканчивающегося конкретными программными продуктами. Часто перед специалистами компаний для повышения эффективности решения задач защиты информации возникает вопрос о выборе соответствующей методики, которая будет удовлетворять адекватным требованиям. Прежде чем осуществлять такой выбор необходимо иметь достаточно полное отображение понятия риска в аспекте информационной безопасности.

В различных публикациях существует множество определений риска [1-45], несущих достаточно широкое его трактование. Только в Интернет-словарях содержится свыше 1500 толкований риска во многих сферах человеческой деятельности [4]. Вследствие этого возникают различные неоднозначности, связанные с раскрытием сущности самого риска и связанных с ним понятий. Соответственно такое состояние характерно и для сферы информационной безопасности.

В этой связи **целью данной работы** является анализ и раскрытие понятия риска, для его последующий интерпретации в области информационной безопасности, это расширит возможности по повышению эффективности решений задач защиты информации.

Учитывая, что риски затрагивают различные предметные области, то это понятие следует рассмотреть с точки зрения безопасности, психологии, экономики, страхования, медицины, геологии и т.д., которое раскрывается как в монографиях, статьях, учебниках, словарях так и различных нормативных, национальных и международных документах.

В большинстве указанных источников риск часто отображается вероятностью или связанными с ней понятиями, например как, **измеряемая или рассчитываемая вероятность:** потерь [4, 10, 33]; появления неблагоприятного исхода [10, 32] или события, (например, в результате которого возможны непредвиденные потери [5, 28]); возможности опасности, неудачи [11], получения результата от принимаемого решения [4, 10], не достижения цели [4], появления обстоятельств обусловливающих неуверенность или невозможность получения ожидаемых результатов от реализации поставленной цели [8]; понести убытки или упустить выгоду (количественно измеряемая неуверенность в получении соответствующего дохода или убытка) [8, 13]; реализации определенной угрозы, вида и величины нанесенного ущерба [10, 20, 22, 45]; причинения вреда имуществу, окружающей среде или жизни (здоровью) граждан, животных, растений [15]; возникновения заданной угрозы и потенциально неблагоприятных последствий возникновения этой угрозы [18]; подразумевающую потенциальную возможность нарушения безопасности [23]; данной угрозы, с помощью которой будут использоваться уязвимости актива или группы активов, чтобы привести к потере и/или повреждению имущества [41]; а также как, сочетание или комбинация вероятности события и его последствий [14, 16, 21, 24, 26, 29, 30, 31].

Известно, что вероятность связанна с наступлением определенного события [7, 12, 39], а соответственно с ним здесь связан и риск, что также видно из выше проведенного анализа публикаций.

Так же в литературе встречается определение риска как **действие или деятельность:** реализация которого ставит под угрозу удовлетворение какой-либо достаточно важной

потребности [1]; состоящая в неопределенности ее исхода и возможных неблагоприятных последствиях в случае неуспеха для субъекта [2, 3]; в том, или ином отношении грозящее субъекту потерей (проигрышем, травмой, ущербом) [2, 25]; в условиях неопределенности и деятельность субъекта, связанная с преодолением неопределённости [4]; наудачу в надежде на счастливый исход [11].

Как известно **действие или деятельность** [39], также как и **вероятность** (измеряемая или рассчитываемая) связаны с возникновениями каких-либо характерных для них событий. Также известно, что любые действия приводят к событиям и последствиям, которые могут представлять собой как потенциальные «положительные» возможности, так и «опасности» [4]. Исходя из сказанного, в этом контексте прослеживается общность указанных понятий.
В отдельных источниках риск трактуется как **мера:** ожидаемого неблагополучия при неуспехе в деятельности, определяемая сочетанием вероятности неуспеха и степени неблагоприятных последствий в этом случае [2]; неопределенности и конфликтности в предпринимательской деятельности [4]; различия между разными возможными результатами принятия определенных стратегий (решениями задачи) [7]; опасности, характеризующая вероятность ее появления и размеры связанного с ней ущерба [6, 12, 19]; возможности реализации опасности в виде определенного ущерба в искусственно созданной действиями субъекта ситуации [34]; возникновения в любой системе нежелательного события с определенными во времени и пространстве последствиями [35].

Здесь видно, что трактование риска также связано с наступлением определенного события, а мера выступает в качестве вторичного фактора и непосредственно связана с количественным или качественным оцениванием.

Следует заметить, что в аналогичном качестве мера имеет место и для **измеряемой или рассчитываемой вероятности,** а также **действия или деятельности.** Мера обычно интерпретируется количественными и качественными показателями, а так же их сочетанием. С философской точки зрения [38] мера рассматривается как взаимосвязь и взаимозависимость количественных и качественных изменений, а в метрологии [39], как средство измерения, предназначенное для воспроизведения и хранения физической величины. Поэтому интерпретация понятия меры относительно определения риска направлена на его отображение (в чем он измеряется) в сочетании «мера риска».

Беря за основу какое-либо определение рассматриваемого понятия, необходимо учитывать, что риск часто характеризуется относительно субъекта деятельности, имеющего определенную цель и воздействующего (или бездействующего) в объективной среде, на события в которой он имеет относительное влияние. Кроме того, риск связан с неопределенностью, необходимостью субъекта использовать аналитические методы и интуицию, а также возможностью получения как положительных, так и отрицательных результатов [4]. Риск определяется как **неопределенность**: например, предполагающая возможность ущерба состояния защищенности интересов (целей) организации банковской системы страны в условиях угроз в информационной сфере [40]; в аспекте контроля и прогноза будущего человеческой деятельности [42].

Встречаются и определения риска, которые отображают его как опасность, ситуацию выбора из двух или **n** вариантов действия. Как **опасность**: предполагаемая (известная); неизвестная на данный момент, но которая может появиться [9, 13]; нанесения ущерба посредством атаки (реализации некоторой угрозы с использованием уязвимости актива или группы активов [17]). **Ситуация выбора** из двух или из **n** вариантов действия (поведения): связанного с возможной неудачей, с одной стороны, и предполагающего хотя бы минимальное сохранение уже достигнутого, с другой [1]; менее привлекательным (однако более надежным) и более привлекательным, (менее надежным, исход которого проблематичен и связан с возможными неблагоприятными последствиями) [2].

Здесь также видно, что рассмотренные понятия риска, которые трактуются как **опасность** (возможность появления какого-либо нежелательного события [12]), **ситуация выбора** из двух или из **n** вариантов действия (поведения) и неопределенность, как и в предыдущих случаях, связаны с наступлением в какой-то **мере** определенного события.

Известны понятия риска, которые определяют его как частоту, величину, характеристику ситуации, событие и т.д., которые напрямую связаны с возникновением того или иного события. Приведем некоторые из них, например, риск как: **частота** реализации «опасности» [36]; как произведение величины события на меру ее возможности [37]; **характеристика ситуации**, с неопределенностью исхода, при наличии неблагоприятных последствий; предположение неуверенности (невозможности получения достоверного знания) о благоприятном исходе в заданных обстоятельствах [10]; **событие**, которое может произойти или не произойти [4] или ожидание наступления **событий** (потенциально нежелательных воздействий на актив или его характеристики, которые могут быть следствием некоторого прошлого, настоящего или будущего события [10, 27]); **затраты или потери** экономического эффекта, связанные с реализацией определенного решения (например, планового варианта) в условиях, иных по сравнению с теми, при которых решение было бы оптимальным [7]. Также риск в любом контексте рассматривается как суммарная величина угрозы (то есть события, которые наносят ущерб), уязвимости (открытость предприятия к угрозам) и стоимости имущества (стоимость актива при опасности). Увеличение любого из этих факторов соответственно увеличивает риски, а снижение ведет к его уменьшению [43].

Таким образом, для исследуемого множества толкований риска можно выделить его базовые характеристики:

- 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 субъекта деятельности событие;
- 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.

Все вышеперечисленные определения в различной мере раскрывают понятие риска и характеризируют его с разных сторон.

После проведенного анализа понятия риска в различных сферах жизнедеятельности человека, можно выделить одну характеристику риска, которая встречается во всех определениях приведенных выше и объединяет их – это событие, которое должно произойти, которое авторы связывают с вероятностью, действием или деятельностью, мерой, частотой, выбором определенных решений, неопределённостью, с потерями, опасностью и т.д.

В аспекте информационной безопасности риск можно связать с событием реализации угрозы ресурсам информационной системы, вследствие которого произошло нарушение одной или более их базовых характеристик безопасности – конфиденциальности, целостности, доступности. Также его, можно описать как: вероятность события, которое привело к нарушению характеристик безопасности; событие которое произошло с участием или без участия субъекта – деятельность или бездействие субъекта; выбор альтернативного варианта; меру; событие, которое происходит с определенной частой; характеристика этого события и т.д.

При раскрытии понятия риска также следует учитывать, что большинство решений по информационной безопасности принимаются в условиях неопределенности [44].

Проведенный анализ показывает, что различные трактования риска имеют общее множество характеристик, например, связь риска с вероятностью и наступлением определенного события и др. Для интерпретации этого понятия в области информационной безопасности необходимо выделить множество его базовых характеристик присущих для этой сферы. В табл. 1 по результатам анализа приведены указанные характеристики, которые были выделены из толкований риска в различных литературных источниках.

Таблица 1

Базовые характеристики риска, отображенные в используемой литературе

Базовые характеристики риска	Номер источника в списке используемой литературы
Вероятность	4, 5, 7, 8, 10, 11, 12, 13, 14, 15, 16, 18, 20, 21, 22, 23, 24, 26, 28, 29, 30, 31, 32, 33, 39, 41, 45
Действие или деятельность	1, 2, 3, 4, 11, 25, 39
Мера	2, 4, 6, 7, 12, 19, 34, 35, 38, 39
Неопределённость	4, 40, 42, 44
Опасность	9, 12, 13, 17
Ситуация выбора	1, 2
Частота	36
Характеристика ситуации	10
Событие	4, 10, 27, 37
Затраты или потери	7
Суммарная величина	43

Список литературы

1 Словарь по психологии [Электронный ресурс] – Режим доступа к словарю: http://www.slovarik.kiev.ua/psychology/r/123726.html

2. Социальная психология. [Электронный ресурс] /Словарь под общей редакцией А.В. Петровского, Л. А.редактор-составитель Карпенко, под ред. М.Ю. Кондратьева // ПЕР СЭ 2005 – Режим доступа к словарю: http://slovari.yandex.ru/dict/psychlex4

3. Азбука социального психолога-практика [Электронный ресурс] / М. Ю. Кондратьев, В. А. Ильин // ПЕР СЭ 2007 – Режим доступа: http://slovari.yandex.ru/dict/azbuka

4. 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

5.Бизнес словарь [Электронный ресурс] – Режим доступа к словарю: http://www.slovarik.kiev.ua/business/r/143514.html

6. Современный экономический словарь [Электронный ресурс] / Б. А. Райзберг, Л. Ш. Лозовский, Е. Б. Стародубцева // Инфра-М – 2006. – Режим доступа к словарю: http://slovari.yandex.ru/dict/economic

7. Экономико-математический словарь [Электронный ресурс] / Л. И. Лопатников – 2003 – Режим доступа к словарю: http://slovari.yandex.ru/dict/lopatnikov

8. Словарь по экономике и финансам. Глоссарий. ру [Электронный ресурс] – Режим доступа к словарю: http://slovari.yandex.ru/dict/glossary

9. Серія «Екологічна безпека» Екологічна безпека України: Системний аналіз перспектив покращення [Электронный ресурс] / А.Б. Качинський – 2001. – РОЗДІЛ 3 // Аналіз ризику – методологічна основа для розв'язання проблем безпеки людини та довкілля – Режим доступа: **http://www.niss.gov.ua/book/Kachin/1-3.htm**

10. Материал из Википедии — свободной энциклопедии [Электронный ресурс] – Режим доступа к словарю: http://ru.wikipedia.org/wiki/Риск

11. Ожегова Словарь [Электронный ресурс] – Режим доступа к словарю:http://www.slovarik.kiev.ua/ojegov/r/103696.html

12. Российская энциклопедия по охране труда [Электронный ресурс] / Общее редактирование Н.И.Маркин // ЭНАС – 2006. – Режим доступа: http://slovari.yandex.ru/dict/trud

13. Международный Институт Исследования Риска [Электронный ресурс] – Режим доступа: http://www.miir.ru

14. Государственный стандарт РФ ГОСТ Р 51897-2002 Менеджмент риска. Термины и определения (принят постановлением Госстандарта РФ от 30 мая 2002 г. N 223-ст) [Электронный ресурс] Risk management. Terms and definitions – Режим доступа: http://sklad-zakonov.narod.ru/gost/Gr51897-2002.htm

15. Национальный Стандарт Российской Федерации стандартизация в Российской Федерации термины и определения Standardization in the Russian Federation. terms and definitions [Электронный ресурс] ГОСТ р 1.12-2004 – Режим доступа: http://narod.yandex.ru/cgi-bin

16. ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements.

17. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

18. ГОСТ Р ИСО/МЭК 15026-2002 Информационная технология. Уровни целостности систем и программных средств. [Электронный ресурс] – Режим доступа: http://www.npo-echelon.ru/common_files/standards.htm

19. Закон України «Про основні засади державного нагляду (контролю) у сфері господарської діяльності» (Відомості Верховної Ради України (ВВР), 2007, N 29, ст.389), 5 квітня 2007 року, N 877-V.

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

21. ISO/IEC Guide 73:2002. Risk management – Vocabulary – Guidelines for use in standards.

22. Информационные системы: оценка рисков [Электронный ресурс] / А.И. Захаров, ведущий специалист по информационной безопасности Securance Technologies, к.т.н. – Режим доступа: http://www.itsec.ru/articles2/actual/inform_sist_ocenka_riskov Опубликовано: Журнал "Information Security/ Информационная безопасность" №6-2005 стр. 18-19.

23. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК-Пресс», 2006. – 320с., ил.

24. ГОСТ Р 51901.1-2002 Менеджмент риска. Анализ риска технологических систем

25. Оксфордский толковый словарь по психологии [Электронный рессурс] /под ред. А.Ребера, – 2002. – Режим доступа: http://vocabulary.ru/dictionary/487/

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

27. Анализ и оценка рисков. [Электронный ресурс] – Режим доступа: http://www.risk24.ru/analiz.htm

28. Глоссарий [Электронный ресурс] – Режим доступа: http://www.glossary.ru

29. ГОСТ Р 51901-2002 Управление надежностью. Анализ риска технологических систем [Электронный ресурс] – Режим доступа: http://zodchii.ws/normdocs/info-2065.html

30. ИСО/МЭК 18045 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Information technology. Security techniques. Methodology for IT security evaluation. [Электронный ресурс] – Режим доступа: http://www.npo-echelon.ru/common_files/gost/GOST-18045-xxxx.pdf

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

32. Fiksel J. Quantitative risk analysis for toxic chemicals in the environment // J. of hazard materials. – 1987. – 10, № 2-3. - P. 227-240.

33. Rowe W. An anatomy of risk. - N.-J.: John Wiley, 1997. – 488 p. 31. U. S. Geological Survey: Proposed procedures for dedealing with warning and preparedness for geologic-related hazard // United States Federal Register. - 1977, 42. №70. - p. 14292-14296.

34. Дзекцер Е. Геологическая опасность и риск (методологическое исследование) // Инженерная геология. – 1992. – № 6. – С. 3-10.

35. Рагозин Ф. Оценка и картографирование опасности и риска от природных и техногенных процессов (теория и методология) // Проблемы безопасности при чрезвычайных ситуациях. - М.: ВИНИТИ, 1993, №5. - С. 16-41.

36. Маршалл В. Основные опасности химических производств. – М.: Мир, 1989. - 672 с.

37. Мушик Э., Мюллер П. Методы принятия технических решений. – М.: Мир, 1990. - 206 с.

38. Новейший философский словарь [Электронный ресурс] / А.А. Грицанов, – 1998. – Режим доступа к словарю: http://terme.ru/dictionary/

39. К. П. Широков. «Большой советской энциклопедии», выпущенной издательством «Советская энциклопедия» в 1969 — 1978 годах в 30 томах. [Электронный ресурс] – Режим доступа к словарю: http://slovari.yandex.ru

40. Стандарт Банка Росии СТО БР ИББС_1.0_2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения.

41. Control Objectives for IT and reated Technology COBIT 4.1 Framework Control Objectives Management Guidelines Maturity Models.

42. Anderson, Alison & Michael Shain. Risk Management: In Caelli, William., Longley, D. & Shain, M. Information Security Handbook. Stockton Press. New York. 1991, pp 75-127.

43. Smith, Martin. Commonsense Computer Security, your practical guide to information security. McGraw-Hill. London. 1993.

44. Taha, Hamdy A. Operations Research. An Introduction. MacMillan Publishing Company. New York. 1987.

45. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Рецензент: д.т.н., проф. Жуков І.А.
Надійшла 25.02.2010 р.