УДК 004.056

В.В. Мохор, д-р техн. наук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев,
А.М. Богданов, д-р техн. наук, ИССЗИ НТУУ «КПИ», г. Киев,
О.Н. Крук, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев,
В.В. Цуркан, ИССЗИ НТУУ «КПИ», г. Киев,
О.В. Цуркан, ИПМЭ им. Г.Е. Пухова НАНУ, г. Киев

АНАЛИЗ КОГНИТИВНОГО ДИССОНАНСА ПОНЯТИЙНОЙ БАЗЫ В СФЕРЕ УПРАВЛЕНИЯ РИСКАМИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Conducted an analysis of cognitive dissonance that arises in the practical application of a number of national standards and recommendations in the field of risk management information security.

Настоящая работа посвящена анализу когнитивного диссонанса, возникающего при практическом использовании ряда отечественных стандартов и рекомендаций в сфере управления рисками безопасности информации. Согласно [1] когнитивный диссонанс есть внутренний психологический, интеллектуальный конфликт, возникающий у индивидуума в результате противоречий между сложившимися представлениями и вновь поступающей информацией. Существование противоречий в понятийной базе, вводимой различными нормативными источниками в сфере информационной безопасности, отмечалось и раньше [2-5]. Постановка задачи, наиболее близкая к настоящей работе, предпринята в [4], где «проведенный объектный анализ выявил недостаточную проработанность понятийного аппарата исследуемого семейства стандартов, проявляющуюся в: (а) неполноте словаря; (б) некорректности некоторых определений; (в) противоречиях между определениями терминов и другими положениями стандартов». Однако попытка анализа понятийной базы безопасности информации с позиций когнитивного диссонанса предпринимается, по нашим сведениям, впервые. При этом отметим, что авторы придерживаются позиции, согласно которой о содержании понятий и терминов не спорят, а договариваются. Однако важно обеспечить непротиворечивость различных договоренностей в отношении одних и тех же терминов и понятий.

Начнем с рассмотрения примеров противоречий. Прежде всего определим систему представлений и категорий, которую мы будем считать установившейся базой построения когнитивных моделей. Примем, что в сфере менеджмента рисков безопасности информации сложившимися представлениями является понятийная база, обусловленная стандартом ISO/IEC Guide 73:2002 “Risk management – Vocabulary – Guidelines for use in standards”[6] и соответствующим ему стандартом ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» [7], а также стандартом ISO/IEC 27005:2005 “Information technology – Security techniques – Information

Security Risk Management" [8] и его переводом на русский язык в виде проекта стандарта ГОСТ Р ИСО/МЭК 27005:2008 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности» [9].

В рамках этой базы определены как сама структура процесса управления рисками безопасности информации, так и термины, принятые для описания различных этапов этого процесса. В частности, стандарты [8, 9] устанавливают, что менеджмент рисков (Risk Management) безопасности информации представляет собой итерационный процесс, который включает следующие этапы:

1. *«Установление контекста» (Context Establishment).*
2. *«Оценка рисков» (Risk Assessment):*
2.1. *«Анализ рисков» (Risk Analysis):*
2.1.1. *«Идентификация рисков» (Risk Identification).*
2.1.2. *«Количественное оценивание рисков» (Risk Estimation).*
2.2. *«Оценивание рисков» (Risk Evaluation).*
3. *«Обработка рисков» (Risk Treatment).*
4. *«Принятие рисков» (Risk Acceptance).*
5. *«Мониторинг рисков» (Risk Monitoring).*
6. *«Коммуникация рисков» (Risk Communication).*

Не останавливаясь на семантических и интенсиональных аспектах русскоязычного перевода англоязычных терминов, отметим важный для дальнейшего факт: стандарты [8, 9] определили, что сущности *«идентификация рисков» (Risk Identification)* и *«количественная оценка рисков» (Risk Estimation)* являются эндогенными, внутренними по отношению к сущности *«анализ рисков» (Risk Analysis)*. В свою очередь, сущности *«анализ рисков» (Risk Analysis)* и *«оценивание рисков» (Risk Evaluation)* являются эндогенными относительно понятия «оценка рисков» *(Risk Assessment)*. Согласно [8, 9] этап обработки рисков *(Risk Treatment)* может быть реализован выбором одной из следующих альтернатив: снижение рисков (Risk Reduction); сохранение рисков (Risk Retention); избегание рисков (Risk Avoidance); перенос рисков (Risk Transfer).

Из этого следует, что сущности *«снижение рисков» (Risk Reduction)*, *«сохранение рисков» (Risk Retention)*, *«избегание рисков»* (*Risk Avoidance*) и *«перенос рисков» (Risk Transfer)* являются внутренним по отношению к сущности *«обработка рисков» (Risk Treatment).* Таким образом, стандарты [8, 9] формируют когнитивную модель иерархии понятий в сфере менеджмента рисков безопасности информации:

Формирование такой иерархии понятий поддерживается толкованиями соответствующих терминов в стандартах [6, 7]. Для примера приведем цитаты толкования понятий, входящих в дерево с корнем «Оценка рисков» (Рис.1.), в соответствии с [7], выстроив их согласно иерархии этого дерева (Рис.1.) и сохраняя стилистику оригинала:

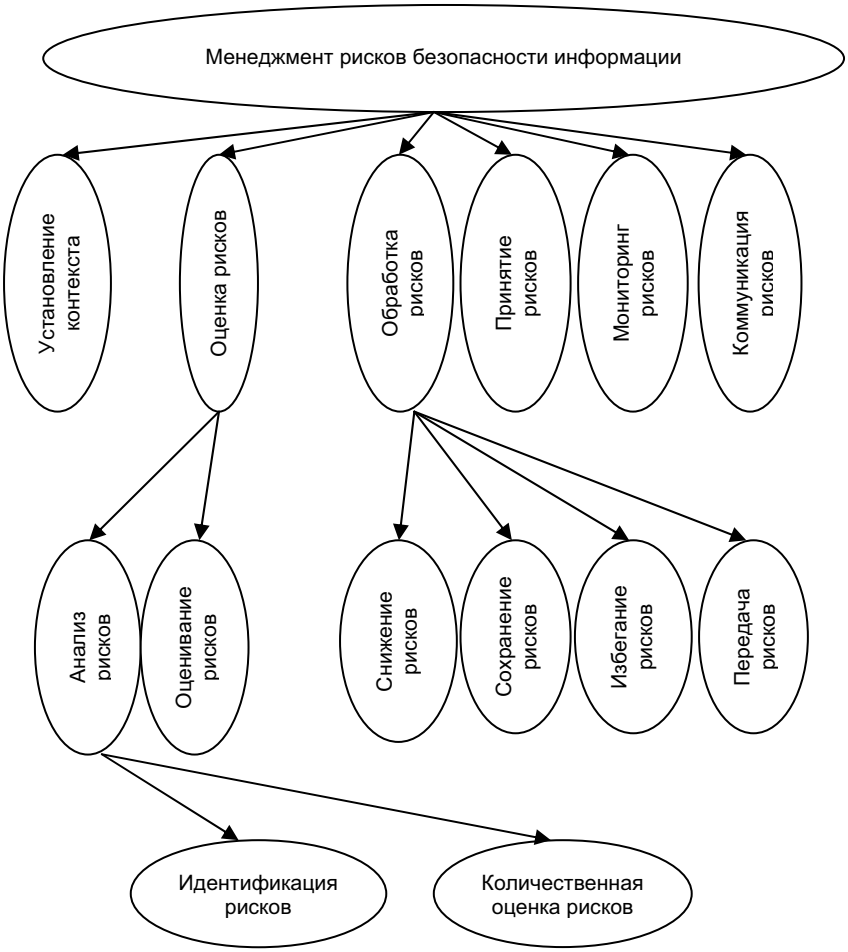

Рис.1. Когнитивная модель иерархии базовых понятий в сфере управления рисками безопасности информации согласно [8, 9]. Стрелки отражают снижение уровня иерархии понятий.

❖ «оценка риска (risk assessment): Общий процесс анализа риска и оценивания риска». (Заметим, что оригинал [6] трактует понятие risk assessment точнее: «Overall process comprising a risk analysis and a risk evaluation», т.е. «Единый процесс, включающий в себя анализ риска и оценивание риска», тем самым явно указывая на эндогенный характер сущностей «анализ риска» и «оценивание риска» относительно сущности «оценка риска»).

➢ «Анализ риска (risk analysis): Систематическое использование

информации для определения источников и количественной оценки риска». (В скобках заметим, что в оригинале [6] речь идет не об определении источников, а об **идентификации рисков**, дословно «systematic use of available information to **identify hazards** and to estimate the risk», а «hazard» и «risk» - это слова-синонимы [10]).

- «Идентификация риска (risk/hazard identification): Процесс нахождения, составления перечня и описания элементов риска».
- «Количественная оценка риска (risk estimation): Процесс присвоения значений вероятности и последствий риска».

➢ «Оценивание риска (risk evaluation): Процесс сравнения количественно оцененного риска с данными критериями риска для определения значимости риска».

Сравнивая иерархию цитированны понятий с иерархией организации этапов процесса менеджмента рисков безопасности информации видим, что обе эти иерархии являются эквивалентными между собой. Поскольку стандарты [6, 7] относятся к сфере менеджмента рисков вообще, а не только к сфере управления рисками безопасности информации, эквивалентность частной иерархии понятий стандартов [8, 9] и общей иерархии понятий стандартов [6, 7] служит подтверждением адекватности когнитивной модели, приведенной на рис.1.

Вопросы управления рисками в той или иной мере отражены во многих отечественных стандартах. Остановимся на некоторых из них.

Рассмотрим ГОСТ Р ИСО/МЭК 13335-1—2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепции и модели менеджмента безопасности информационных и телекоммуникационных технологий» [11]. Толкования понятийной базы этого стандарта имеют отличия от «сложившихся представлений», принятых нами. Процитируем толкования терминов, которые привлекли внимание:

- «оценка риска (risk assessment): Процесс, объединяющий идентификацию риска, анализ риска и оценивание риска»;
- «анализ риска (risk analysis): Систематический процесс определения **величины** риска».

Хотя в [7] указано, что «в настоящем стандарте приведены термины по ИСО/МЭК 17799, ИСО/МЭК 13335-4, а также следующие термины с соответствующими определениями», содержание понятий «идентификация риска», «оценивание риска» и «определение величины риска» не раскрыты ни в одном из них. Таким образом, мы должны строить свою когнитивную модель иерархии этих понятий, исходя из поступившей информации и представлений, сложившихся у нас ранее. Анализируя содержание сущности «анализ риска», предписанное [11], мы должны сделать вывод, что оно тождественно сущности «величина риска» в некотором «систематическом процессе» ее определения.

Пытаясь определиться с толкованием сущности «определение величины риска» исходя из имеющихся у нас представлений, мы методом исключения приходим к выводу, что «определение величины риска» в смысле стандарта [11] есть то же самое, что и «количественная оценка риска» в смысле стандартов [6-9].

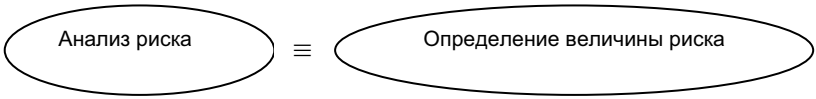

Рис. 2. Когнитивная модель сущности «анализ риска» по стандарту [11]

Следовательно, когнитивная модель, представленная на рис.2, приводит к когнитивному диссонансу, т.к. в базе наших убеждений зафиксировано, что «анализ риска» – это «идентификация риска» плюс «количественная оценка риска». Возникает вопрос, как избавиться от диссонанса? Этого можно добиться, если в толковании сущности «оценка риска» по стандарту [11] вместо термина «анализ риска» использовать термин «количественная оценка риска». При этом мы получим следующее толкование: «оценка риска (risk assessment): Процесс, объединяющий идентификацию риска, количественную оценку риска и оценивание риска». Такая формулировка позволяет нам агрегировать сущности «идентификация риска» и «количественная оценка риска» в некоторую отдельную, безымянную сущность, соответствующую ранее существующим у нас представлениям о сущности «анализ рисков» в смысле [6-9]. Тогда для сущности «оценка риска» мы можем рассмотреть две когнитивные модели (Рис.3.).

Видим, что одна из этих моделей (а именно, левая) является моделью с когнитивным диссонансом (сущность «идентификация риска» оказалась на одном уровне иерархии с сущностями «анализ риска» и «оценивание риска»). Ранее сложившаяся у нас система представлений требует, чтобы понятия «анализ риска» и «оценивание риска» находилось на более высоком уровне иерархии, чем понятие «идентификация риска».

Другая модель (правая) не содержит когнитивного диссонанса, ибо в ней сущности «идентификация риска» и «количественная оценка риска» являются эндогенными по отношению к некоторой безымянной сущности, уровень иерархии которой равен уровню иерархии сущности «оценивание риска». Это означает, что для устранения когнитивного диссонанса нам нужно исключить термин «анализ риска» из текста стандарта [11], заменив его термином «количественная оценка риска». Анализ текста [11] показал, что выполнение такой замены не сказывается ни на общей сути стандарта, ни на каких либо самых тонких нюансах его содержания.

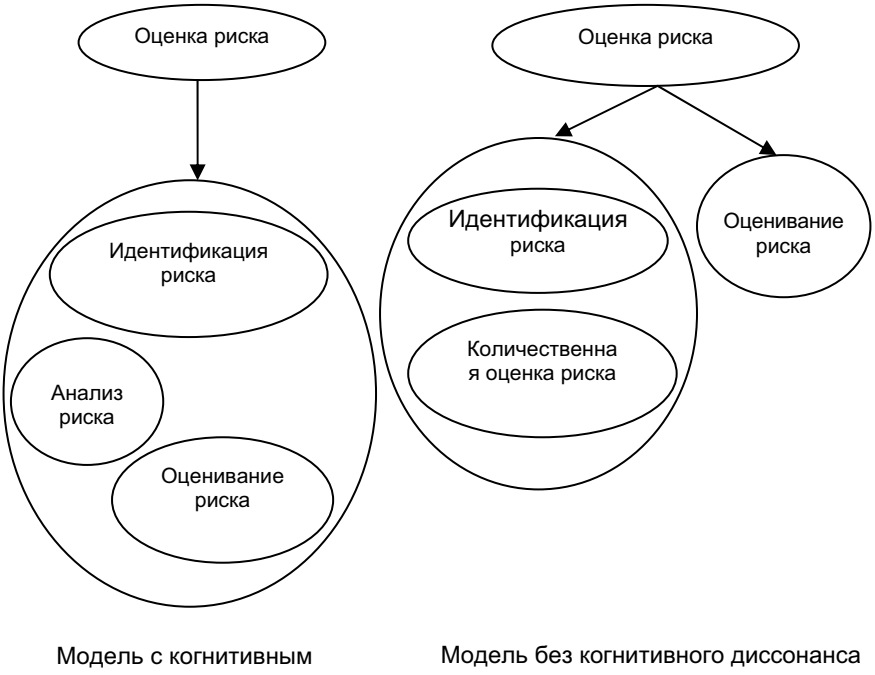

Рис.3. Когнитивные модели сущности «оценка риска» по стандарту [11].

Рассмотрим стандарт ГОСТ Р ИСО/МЭК ТО 13335-3 – 2006 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий» [12]. Часть 3 этого стандарта «Термины и определения» состоит из одного короткого предложения: «В настоящем стандарте применены термины по ИСО/МЭК 13335-1». Выше мы рассмотрели, что понятийная база стандарта ИСО/МЭК 13335-1 приводит к когнитивному диссонансу в отношении понятия «анализ риска» и можно предположить, что этот термин будет вызывать диссонанс и при формировании когнитивных моделей в контексте стандарта [12].

Анализ текста стандарта [12] показал, что система понятий, используемых в нем, предполагает построение когнитивной модели, кардинально отличающейся от модели по [6-9]. Наглядным примером и частным доводом в подтверждение данного тезиса служит когнитивная модель иерархии понятий с корнем в узле «анализ рисков», построенная на основе раздела 9 и рисунка на стр.12 стандарта [12].

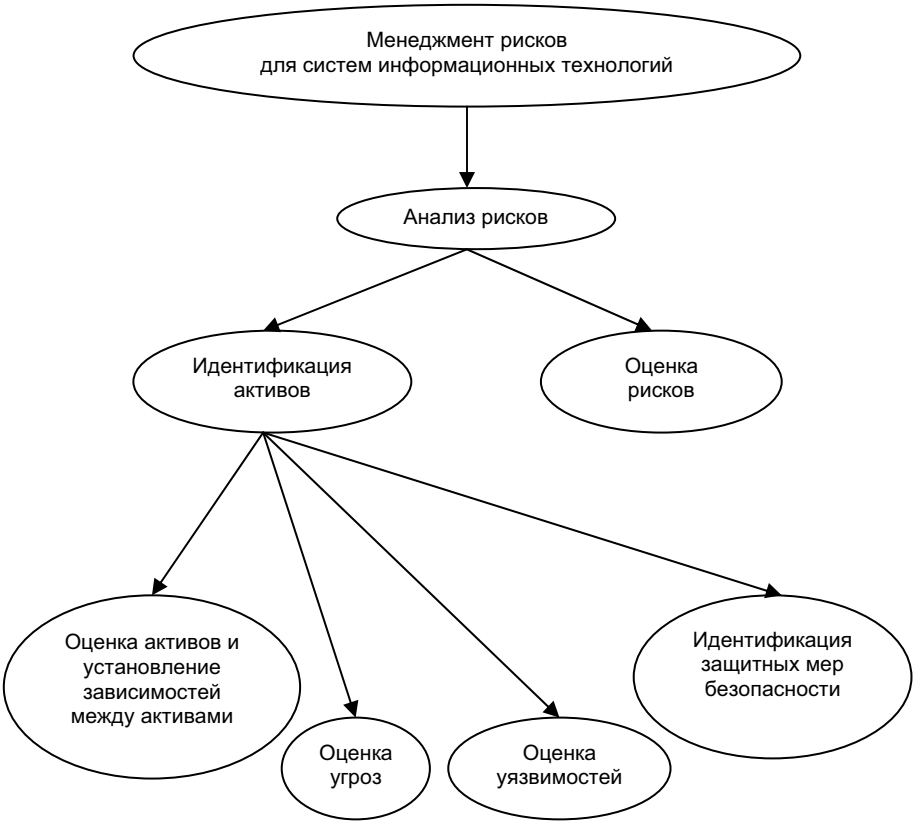

Рис.4. Когнитивная модель иерархии понятий в сфере управления рисками по ветви «анализ рисков» согласно стандарту [12]

Сравнивая когнитивную модель сложившейся системы представлений (Рис.1) и модель на Рис.4, видим, что иерархия понятий стандарта [12] противоречит иерархии понятий, сложившихся на основе [6-9]. Прежде всего это проявляется в том, что сущность «оценка рисков» в базовой модели имеет более высокую степень иерархии по сравнению с сущностью «анализ рисков». В модели же по стандарту [12] наоборот, иерархия сущности «анализ рисков» превышает иерархию сущности «оценка рисков». Это означает, что диссонанс невозможно устранить способом, использованным при согласовании когнитивной модели стандарта [11], т.е. исключением термина «анализ риска» и заменой его на термин «количественная оценка риска». Т.о. нужно строить абсолютно иную когнитивную модель процесса менеджмента безопасности информации, используя при этом ту же самую семиотическую систему терминов.

Отмеченная коллизия находит свое продолжение в стандартах [13, 14]. В результате мы приходим к необходимости всякий раз при обсуждении вопросов безопасности информации делать ссылку на группу стандартов, которую мы подразумеваем в качестве базы нашей когнитивной модели.

Рассмотрим в качестве следующего примера «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения» [15]. Во введении к данному документу указано, что «стандартизованные термины набраны полужирным шрифтом, их краткие формы, представленные аббревиатурой, - светлым, а синонимы – курсивом». Смотрим пункт 3.5.19 и видим: «Оценка риска; *анализ риска*: Выявление угроз безопасности информации, уязвимостей информационной системы, оценка вероятностей угроз с использованием уязвимостей и оценка последствий реализации угроз для информации и информационной системы, используемой для обработки этой информации». Из этого толкования следует, что понятия «оценка риска» и «анализ риска» являются синонимичными. В этом же пункте явно указано, что понятия *risk assessment* и *risk analysis* являются синонимами. Дополнительно это подтверждается алфавитным указателем, где понятиям «оценка риска», «анализ риска», «risk assessment» и «*risk analysis*» поставлена в соответствие одно и то же толкование – п.3.5.19. Иными словами, рекомендации [15] предписывают следующую когнитивную модель:

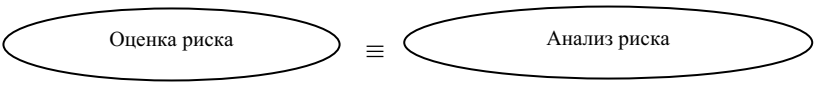

Рис.5. Когнитивная модель эквивалентности сущностей «оценка риска» и «анализ риска» в соответствии с [15]

Очевидно, что эта когнитивная модель не совпадает ни с одной из ранее рассмотренных моделей.

Приведенные примеры показывают, что понятийная база в сфере безопасности информации настолько противоречива, что в ней возможны любые возможные взаимно исключающие варианты трактовки тех или иных сущностей. Вследствие этого попытки решать задачи управления рисками безопасности информации с опорой на отечественную базу понятий и терминов в данной сфере, регламентированных какими-либо стандартами, будут автоматически приводить к обязательному несоответствию каким-нибудь другим стандартам из этой же сферы.

В каких направлениях следует искать выход из сложившейся ситуации? Если отечественную понятийную базу в сфере безопасности информации рассматривать как информационный актив, то вышеприведенный анализ показывает, что этот актив сам подвержен рискам информационной безопасности (очевидно, по категории «целостность информации»). Следуя теории управления рисками, можем определить четыре возможных направления их обработки: сохранение, уменьшение, перенос, избегание.

1. В рассматриваемом контексте сохранению, удержанию рисков соответствует тактика согласия с существующим состоянием понятийной базы стандартов. Следствием этой тактики является несоответствие любого из решений каким-нибудь стандартам. Очевидно, что такая тактика не является оптимальной для реальной практики.

2. Уменьшению рисков может соответствовать построение в каждом конкретном случае системы дополнительных согласований и интерпретаций, обеспечивающих снятие противоречий относительно используемых стандартов и исключение из рассмотрения тех задач, которые подразумевают использование стандартов с иными трактовками базовых понятий. Такое решение требует, очевидно, выполнение большого объема повторяющейся и, в определенном смысле, бесплодной работы.

3. Избеганию рисков будет отвечать позиция полного игнорирования задачи управления рисками, отрицание ее актуальности на данном этапе и/или в данных условиях. Можно предположить, что превалирующее в реальной практике управления информационной безопасностью стремление к игнорированию задач менеджмента рисков является проявлением тактики избегания, избираемой в том числе и вследствие когнитивного диссонанса понятийной базы спектра основных стандартов в этой сфере.

4. Переносу рисков соответствует передача решения задач в сфере менеджмента рисков третьим организациям с возложением на них ответственности за разрешение всех возникающих противоречий. Такой путь является единственно конструктивным для видов деятельности, при которых в силу различных объективных обстоятельств не может быть использована тактика избегания.

Согласно [1] дискомфорт или напряжение, вызванные конфликтом когнитивного диссонанса, могут быть устранены при помощи одного из нескольких защитных действий: индивид отвергает или избегает новой информации, или убеждает себя, что противоречия на самом деле не существует, или примиряет противоречия, или прибегает к другим мерам с целью сохранения стабильности и порядка в своем представлении о мире и о себе. В контексте сказанного видим, что вышеназванные четыре направления обработки риска понятийных противоречий в отечественной понятийной базе в сфере управления безопасностью информации перекрывают все возможные варианты разрешения конфликта когнитивного диссонанса.

В заключение отметим, что с принятием в конце 2009 года нового стандарта ISO 31000 «Risk management — Principles and guidelines», всецело посвященного управлению рисками и предпринимающего попытку «навести порядок» в этой сфере, следует ожидать появления и соответствующего отечественного стандарта. Остается надеяться, что при отечественной локализации ISO 31000 будет системно решена задача уменьшения рисков когнитивного диссонанса понятийной базы в сфере безопасности вообще и безопасности информации в частности.

1. *Философский* энциклопедический словарь/ Гл. редакция: Л.Ф.Ильичев, П.Н.Федосеев, С. М. Ковалев, В. Г. Панов – М.: Сов. Энциклопедия, 1983. –840 с.
2. *Храмцовская Н.* Стандарты ИБ: ищем ошибки в новом госте. –http://safe.cnews.ru/reviews/index.shtml?2007/01/10/230553_1.
3. *Цирлов В., Марков А.* Управление рисками – нормативный вакуум информационной безопасности. – http://www.osp.ru/os/2007/08/4492873/ prinver.htm
4. Черемушкин Д.В. Корректировка стандартов семейства ISO/IEC 27000 на основе объектной модели словаря // Сборник трудов конференции молодых ученых, Выпуск 6. Информационные технологии.– СПб: СПбГУ ИТМО, 2009. – С. 43-48.
5. *Мохор В.В., Цуркан В.В.* Атестування ризику безпеки інформації в організаційно-технічних системах об'єктів інформаційної діяльності // XIII Международная научно-практическая конференция «Безопасность информации в информационно-телекоммуникационных системах», 18-21 мая 2010 г., тезисы докладов. – К.: ЧП «ЕКМО», НИЦ «ТЕЗИС» НТУУ «КПИ», 2010. – С.69-70.
6. *ISO/IEC Guide 73:2002* "Risk management – Vocabulary – Guidelines for use in standards".
7. *ГОСТ Р 51897-2002* «Менеджмент риска. Термины и определения». – http://www.complexdoc.ru/text/ГОСТ Р51897-2002
8. *ISO/IEC 27005:2005* "Information technology – Security techniques – Information Security Risk Management".
9. *Проект ГОСТ Р ИСО/МЭК 27005:2008* «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности». – http://docs.cntd.ru/document/1200075254/
10. *Англо-русский словарь*. 70 000 слов и выражений. Изд. 15-е стереотип./Сост. В.К.Мюллер. – М.: Сов. энциклопедия, 1970. – 912 с.
11. *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». – М.: Стандартинформ, 2007. – 18 с.
12. *ГОСТ Р ИСО/МЭК ТО 13335-3 —2007* «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий». – М.: Стандартинформ, 2007. – 46 с.
13. *ГОСТ Р ИСО/МЭК 13335-4 – 2007* «Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер». – М.: Стандартинформ, 2007. – 62 с.
14. *ГОСТ Р ИСО/МЭК ТО 13335-5 – 2006* «Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети». – М.: Стандартинформ, 2007. – 23 с.
15. *Р 50.1.056-2005* «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения». – М.: «Стандартинформ», 2006.

Поступила 15.09.2010р.