

И. Н. Васильева, Е. В. Стельмашонок. Современный взгляд на управление информационной безопасностью предприятия // Вестник СПбГЭУ. Серия "Экономика". — 2014. — Вып. 1 (68). — С. 166-171.

УДК 65.01

Васильева Ирина Николаевна,

доцент, к.ф.-м.н.;

Стельмашонок Елена Викторовна,

профессор, д.э.н.,

Санкт-Петербургский государственный экономический университет;

e-mail: dept.kvsip@engec.ru

Современный взгляд на управление информационной безопасностью предприятия

В статье рассматриваются современные подходы к организации и управлению деятельности по обеспечению корпоративной информационной безопасности.

Ключевые слова: информационная безопасность, риск, процесс, стратегическое управление, менеджмент

Vasileva Irina Nikolaevna,

Docent, Ph.D.;

Stelmashonok Elena Viktorovna,

Professor, Doctor of Economics;

St. Petersburg State University of Economics;

Modern view of enterprise information security management and governance

The paper deals with modern approaches to organizing and managing activities to ensure corporate information security.

Keywords: information security, risk, process, governance, management

Управление информационной безопасностью (ИБ) предприятия необходимо для определения потребности предприятия в обеспечении информационной безопасности, правильного перераспределения ресурсов и совершенствования деятельности в сфере ИБ для обеспечения устойчивого функционирования корпоративной информационной инфраструктуры и достижения бизнес-целей компании.

Общепринятым подходом является внедрение на предприятии системы менеджмента информационной безопасности (СМИБ), базирующейся на стандартных моделях и принципах. Большинство «лучших практик» обеспечения ИБ, оформленных в ряде национальных и международных стандартов, а также в документах профессиональных сообществ в этой сфере, базируются на процессном подходе, замкнутом цикле менеджмента PDCA и бизнес-модели информационной безопасности предприятия. Наиболее известными документами являются

международные стандарты ISO/IEC серии 27000 на СМИБ (и принятые в России гармонизированные ГОСТы), национальные стандарты Великобритании (серия BS 7799), Германии (серия BSI 100) и США (серия NIST 800), а также стандарты международной ассоциации аудиторов информационных систем ISACA (Cobit) и консорциума ISM3 (ISM3).

Процессный подход к организации и управлению хозяйственной деятельностью предприятия обуславливает необходимость применения процессно-ориентированного подхода и к формированию корпоративной инфраструктуры защиты информации. Это позволяет рассматривать процесс обеспечения ИБ предприятия, то есть формирование и развитие системы защиты информации, как один из вспомогательных (инфраструктурных) процессов, обеспечивающих основные бизнес-процессы предприятия (Рис.1). Таким образом, процессный подход дает возможность разработки инфраструктуры защиты информации в тесной взаимосвязи с проектированием других бизнес-процессов, что, несомненно, позволяет повысить их интегрированность, гибкость, сбалансированность и управляемость.

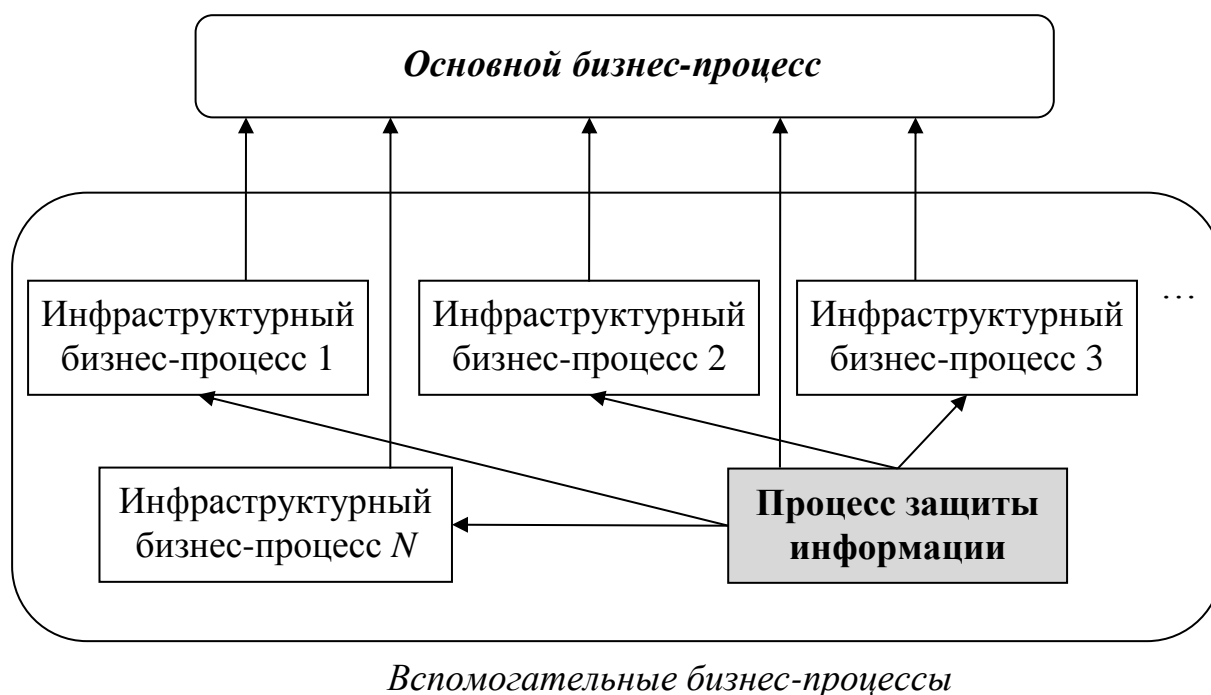


Рис.1. Влияние процесса защиты информации на другие бизнес-процессы

С другой стороны, информационная инфраструктура предприятия должна рассматриваться как основа бесперебойного функционирования бизнес-процессов. Любая используемая в бизнесе техническая система, являясь важным элементом инфраструктуры, должна предоставлять бизнесу определенный тип сервиса. Сервис заключается в предоставлении

бизнесу необходимой информации нужного качества, в нужное время и в нужном месте, то есть, в конечном итоге, информации для управления самим бизнесом. При этом технология управления уровнем сервиса, предоставляемого информационной инфраструктурой, позволяет перейти от технического подхода к бизнес-ориентированному. Для сервисного подхода характерен акцент на обязательства и взаимодействие, управление результатами.

Сервисный подход позволяет отразить требования бизнеса к ИБ в соглашениях об уровне сервиса для ИТ-систем, при этом одним из наиболее важных показателей является доступность сервиса. В таком контексте задачей процесса управления ИБ является постоянное обеспечение безопасности услуг на согласованном с партнером уровне, а сама информационная безопасность является важнейшим показателем качества управления [7].

Эволюция восприятия информационных технологий – от сервисной функции к движущей силе изменений и развития бизнеса («инновационность» бизнеса) [1] предъявляет повышенные требования к защищенности информационной инфраструктуры, предоставляющей бизнесу доверенную и безопасную среду.

Структура системы обеспечения информационной безопасности предприятия состоит из двух компонентов:

- система управления ИБ,
- система защиты информации, собственно реализующая процессы ИБ.

Система защиты информации непосредственно обеспечивает конфиденциальность, целостность и доступность информационных активов. Она состоит из множества различных процессов, таких как контроль доступа, реагирование на инциденты безопасности, защита от внутренних и внешних атак, безопасная разработка программного обеспечения, обучение и повышение осведомленности персонала по вопросам ИБ, управление изменениями и т.п., каждый из которых направлен на обработку определенных рисков. Количество процессов системы защиты информации определяется зависимостью бизнеса от информационных технологий и масштаба ее информационной инфраструктуры, и в среднем составляет порядка 10 самостоятельных процессов, хотя в отдельных случаях их количество может достигать 20 и более.

Сервисный подход обычно применим именно к системе защиты информации, то есть к уровню операционной деятельности по обеспечению ИБ, охватывающему технические и организационные процессы и процедуры защиты информации. Такой подход нашел отражение в руководстве Cobit 5 for Information Security [8], операционный уровень в котором представлен сервисами безопасности.

Международные стандарты ISO определяют систему управления ИБ как часть общекорпоративной системы менеджмента, базирующуюся на оценке бизнес-рисков, необходимую для создания, внедрения, функционирования, мониторинга, пересмотра, поддержки и улучшения информационной безопасности. При этом под словом «система» в СМИБ ISO понимает скорее процесс, программу действий или методологию. СМИБ объединяет воедино людей (персонал), процессы и ИТ-системы, обеспечивая слаженную работу службы безопасности, ИТ-отдела и руководства компании.

Согласно ISO/IEC 27001 [2] СМИБ включает четыре основных процесса менеджмента (цикл PDCA): планирование (Plan), внедрение (Do), мониторинг (Check) и совершенствование (Act). При этом формирование СМИБ базируется на следующих основных принципах:

- приверженность руководства (СМИБ может быть создана только руководством компании, которое распределяет зоны ответственности и контролирует выполнение обязанностей);
- вовлеченность в процесс обеспечения ИБ всех сотрудников, имеющих дело с информационными ресурсами (обучение и повышение осведомленности сотрудников, обеспечение взаимодействия по вопросам ИБ, формирование корпоративной культуры ИБ);
- оценка рисков (отсутствие в организации процессов управления рисками приводит к неадекватности принимаемых решений и неоправданным расходам).

Стандарты управления рисками [3,9] обращают внимание на необходимости систематического подхода к управлению рисками ИБ и на согласованности этого подхода с общим подходом к управлению рисками в масштабе организации.

Управление рисками должно быть неотъемлемой частью всех видов деятельности, связанных с управлением ИБ, и осуществляться как на этапе внедрения (циклы планирования и реализации), так и на этапе текущего функционирования (циклы контроля и совершенствования) СМИБ.

Единые нормы корпоративного управления, общие подходы к анализу риска позволяют значительно снизить как внутренние затраты предприятия, так и стоимости работ по внедрению и сертификации различных систем менеджмента (качества, экологической безопасности, ИБ). При этом крайне важным является общая нацеленность на достижения бизнес-целей организации.

Современные модели управления корпоративной ИБ делают акцент на достижение бизнес-целей и согласование целей ИБ с потребностями бизнеса. Любое предприятие существует для того, чтобы создавать некоторую ценность для заинтересованных сторон (владельцев, акционеров, пользователей, органов власти, подрядчиков, заказчиков и

общества в целом). Поэтому задача стратегического управления любым предприятием – коммерческим или государственным – формирование ценности, что подразумевает получение выгоды за счет оптимизации стоимости ресурсов и оптимизации рисков. Эти потребности заинтересованных сторон должны быть преобразованы в действенную, реализуемую на практике стратегию компании.

Выделение в организации деятельности предприятия нескольких уровней (организация в целом, бизнес-процессы, информационные системы) и организация межуровневого взаимодействия [9] позволяет связать бизнес-риски (цели бизнеса), задачи управления и информационную инфраструктуру (Рис.2).

Такой многоуровневый подход, нашедший отражение в документах ISM3 [5,10] и Cobit 5 for Information Security, позволяет сформировать каскад целей ИБ (Рис.3), избежать сугубо технического понимания и уйти от самодостаточности этой области деятельности, нацелив ИБ на предоставление качества и ценности для бизнеса.

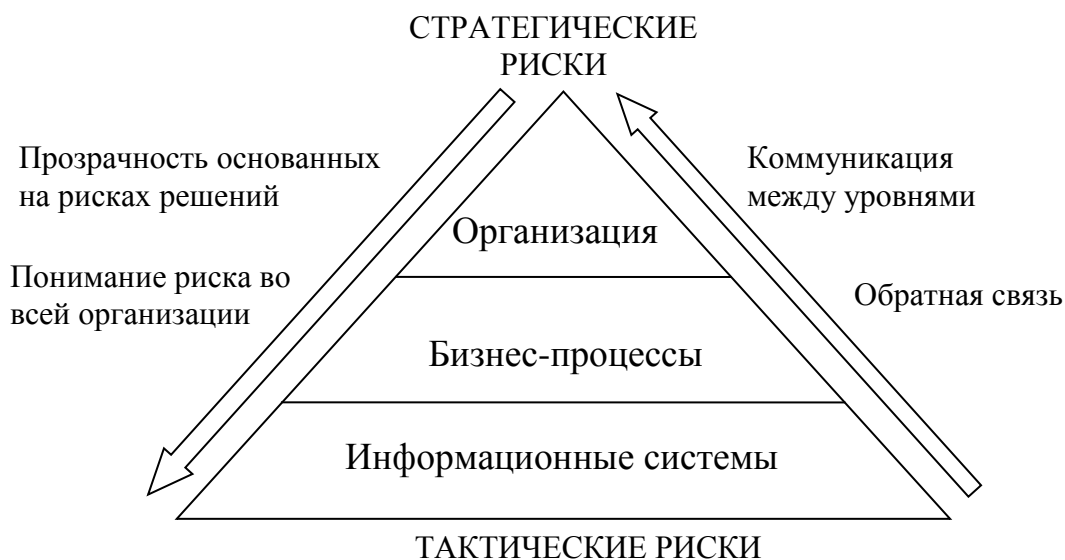


Рис.2. Многоуровневое управление рисками на предприятии

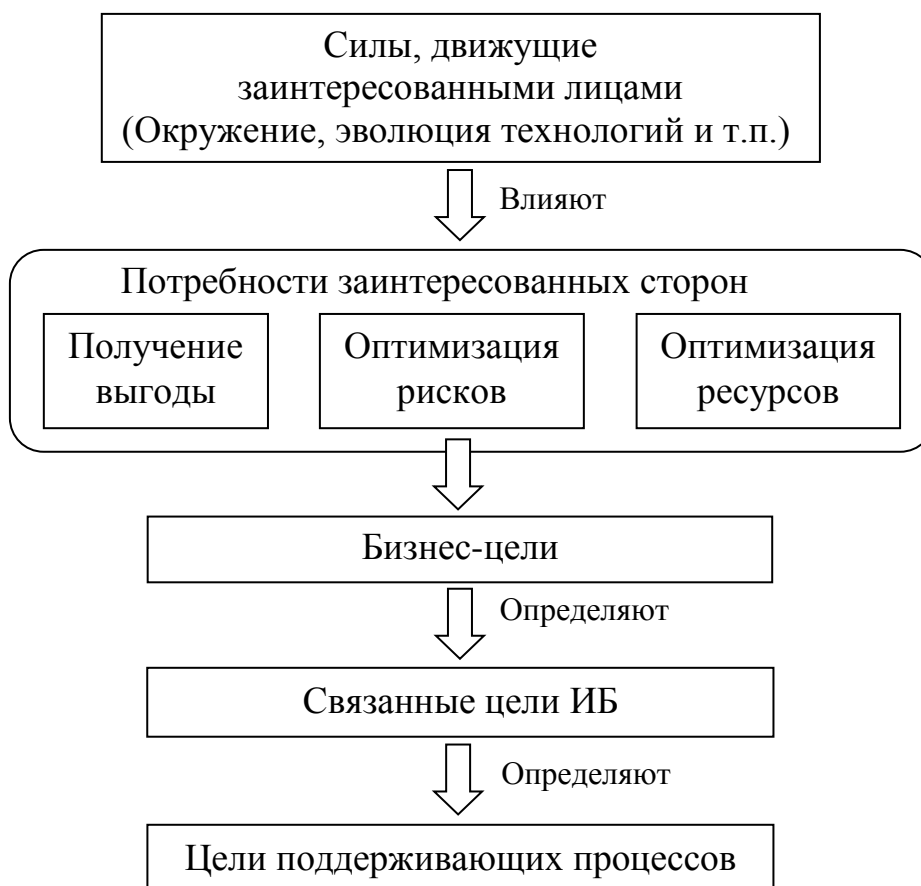


Рис.3. Каскад целей ИБ согласно Cobit 5

Управление ИБ в организации также является многоуровневым и определяется, в конечном счете, потребностями бизнеса. Важным принципом, характерным для современных моделей управления ИБ, является разграничение зон стратегического (Governance) и текущего управления (Management). Принцип разграничения стратегического и текущего управления предполагает не полное их разделение, а согласованное действие с разграничением функций и зон ответственности (Рис.4).

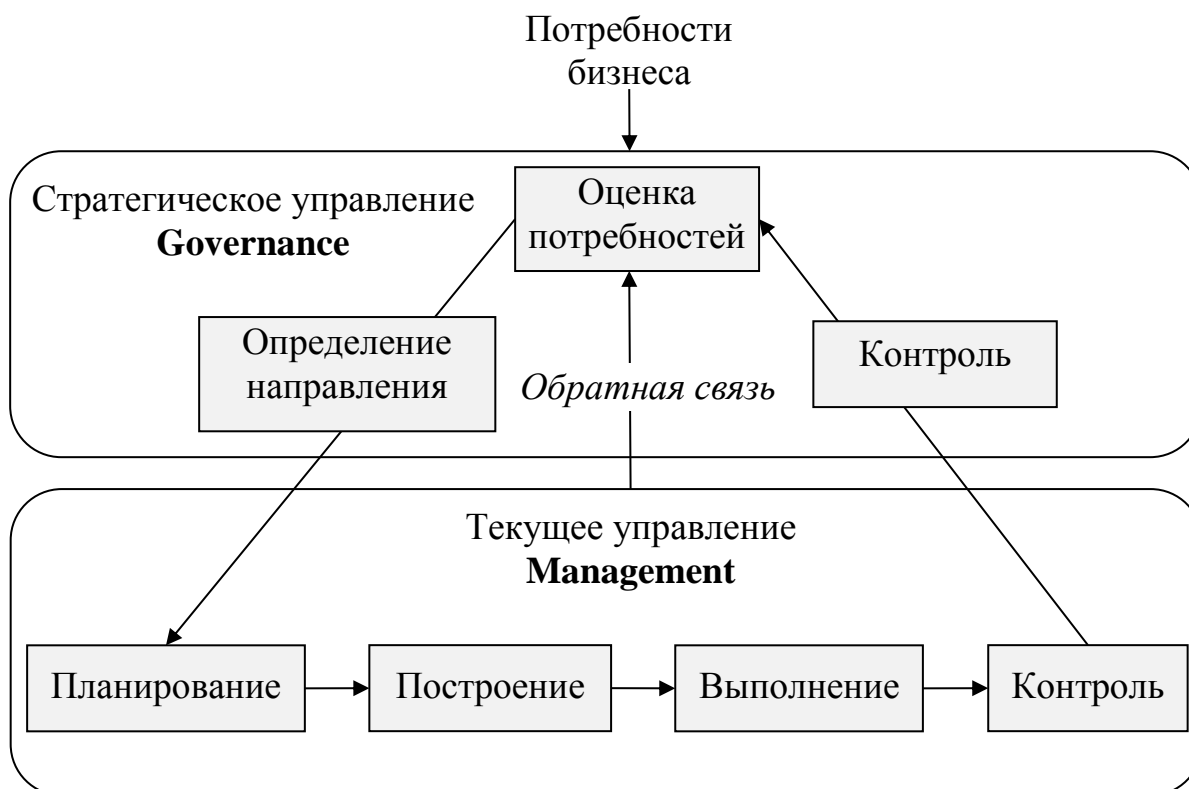


Рис.4. Разделение уровней управления Cobit 5

Под стратегическим управлением (корпоративным управлением) понимается управление на уровне высшего руководства, направленное на достижение бизнес-целей предприятия. В сферу стратегического управления, согласно Cobit 5, входят:

- Оценка потребностей всех заинтересованных сторон, условий и возможностей (Evaluate);
- Определение стратегического направления путем расстановки приоритетов и принятия решений (Direct);
- Контроль продуктивности, выполнения требований и решения задач в рамках выбранного направления (Monitor).

В области стратегического управления Cobit 5 определяет следующие процессы:

- Обеспечение определения модели и поддержки руководства;
- Обеспечение ценности;
- Обеспечение оптимизации рисков;
- Обеспечение оптимизации ресурсов;
- Обеспечение прозрачности для заинтересованных лиц.

В сферу текущего управления (менеджмента) входят: планирование (Plan), построение (Build), выполнение (Run) и проверка (Monitor) отдельных видов деятельности в соответствии со стратегическим

направлением, установленным высшим руководством компании для достижения бизнес-целей. Уровень текущего управления Cobit 5 соответствует, с некоторыми изменениями, модели непрерывного совершенствования PDCA.

Концепция Governance, подобная рассмотренной выше, описывается проектом стандарта ISO/IEC 27014 Governance of Information Security, посвященного корпоративному управлению ИБ [4]. В стандарте ISO/IEC 27014 выделяются следующие пять основных областей охвата системы корпоративного управления ИБ:

- согласованность стратегии ИБ и бизнеса,
- оценка эффективности,
- менеджмент рисков,
- управление ресурсами и
- увеличение стоимости.

Таким образом, стратегическое управление ИБ обеспечивает связь между бизнесом и ИБ, выступая как связующее звено между менеджментом ИБ, инициативами соответствия (compliance), управлением рисками и корпоративной бизнес-стратегией. Рассмотренная связь нашла отражение еще в одной концепции – GRC (Governance, Risk, Compliance). Эффективная модель GRC включает персонал, процессы, технологии и организационные факторы [11].

Концепция GRC крайне актуальна и для ИБ. Несогласованность ИБ со стратегическими целями бизнеса и недостаточное осознание проблем ИБ со стороны руководства зачастую приводит к нехватке бюджетов на необходимую защиту, перерасходу на решение неактуальных задач и потерям, связанным с происходящими инцидентами. Основа GRC – это доведение до сведения высшего руководства информации о рисках и исполнении требований, а информационная безопасность как раз и занимается снижением информационных рисков и исполнением требований отраслевых стандартов.

Все вышесказанное позволяет выделить в организации деятельности по обеспечению ИБ предприятия несколько уровней (Рис.5).

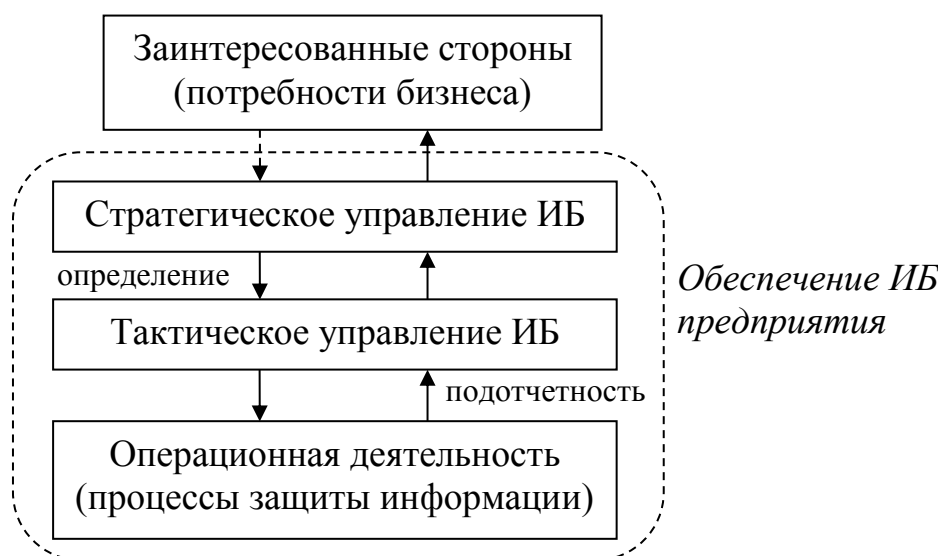


Рис.5. Уровни деятельности по обеспечению ИБ предприятия

Процессы управления выполняются беспрепятственно сквозь все три уровня с целью непрерывного совершенствования деятельности и обеспечения эффективного межуровневого и внутри уровневого взаимодействия.

На современном этапе развития управления ИБ осознана необходимость дальнейшего приближения проблем ИБ к результатам бизнес-деятельности (конечному продукту) предприятия. Актуальная модель ИБ объединяет стратегию и строение предприятия, людей (персонал), процессы и технологии, взаимодействующие между собой и вносящие свой вклад для достижения общей цели [6].

Характерными чертами такой модели ИБ являются:

- акцент на формирование ценности для бизнеса,
- многоуровневое управление и разграничение зон стратегического и текущего управления.

При этом цели ИБ должны быть увязаны с основными бизнес-целями компании, реализован риск-ориентированный подход к обеспечению ИБ, а система управления ИБ должна быть интегрирована в общекорпоративное управление не как изолированная и независимая система процессов, а как его неотъемлемая, сильно связанная составная часть.

Такая модель ИБ отвечает реальным интересам бизнеса, напрямую способствуя результативности и необходимому улучшению основной деятельности предприятия за счет создания и поддержания безопасной и доверенной информационной среды.

Литература

1. Голубев В. COBIT 5 - что нового? 06.06.2012. URL: http://itsmforum.ru/news/all_news/2012_06_06/4_COBIT5-

- Novaya_versiya___novoe_soderzhanie_Viktor_Golubev.pdf (дата обращения: 30.10.2013).
2. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. – М.: Стандартинформ, 2008. – 26 с.
 3. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности – М.: Стандартинформ, 2011. – 46 с.
 4. Курило А.П., Голованов В.Б. Созидатели стандарта // Информационная безопасность банков. BIS-Journal. Отраслевой интернет-журнал. 26.07.2011. URL: <http://www.journal.ib-bank.ru/pub/63> (дата обращения: 26.11.2013).
 5. Aceituno V. ISM3: A Standard for Information Security Management//ISSA Journal. October 2006. – P.22-25.
 6. An Introduction to the Business Model for Information Security. ISACA, 2009. URL: <http://www.isaca.org/Knowledge-Center/Research/Documents/Intro-Bus-Model-InfoSec-22Jan09-Research.pdf> (дата обращения: 01.11.2013).
 7. BS ISO/IEC 20000 – процессный подход к управлению информационной безопасностью современной организации. URL: http://www.itsmonline.ru/phparticles/show_news_one.php?n_id=286 (дата обращения: 01.09.2013).
 8. Cobit 5 for Information Security Introduction. URL: <http://www.isaca.org/COBIT/Documents/COBIT-5-for-Information-Security-Introduction.pdf> (дата обращения: 29.08.2013).
 9. Managing Information Security Risk. Organization, Mission, and Information System View. NIST. Special Publication 800-39. – USA, 2011. URL: <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf> (дата обращения: 08.11.2013).
 10. Open Information Security Management Maturity Model (O-ISM3). URL: <https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12238> (дата обращения: 02.11.2013).
 11. Sam Jr. ECM as a Foundation for GRC. 30.11.2010. URL: <http://paperfreetech.com/ecm-as-a-foundation-for-grc/> (дата обращения: 12.09.2013).