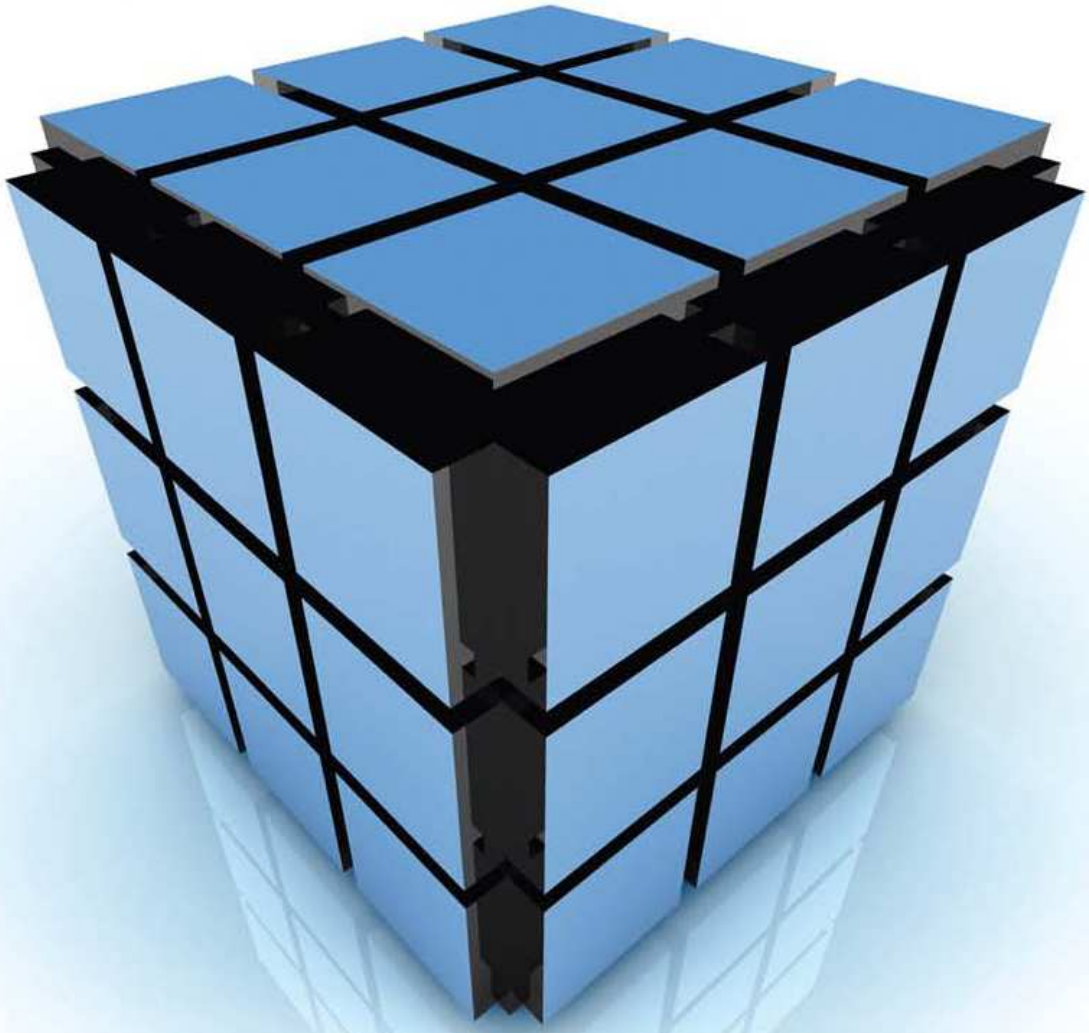
Как успешно пройти сертификацию по 27000

Пример применения Compliance Management'a



Sigurjon Thor Arnason · Keith D. Willett

Auerbach Publications
Taylor & Francis Group

Предисловие

Введение

Глава 1. Введение в стандарты ISO по безопасности

Эта глава предполагает, что читатель хотя бы в общем знаком с информационной безопасностью, знает, что это такое, а также потенциальные применение информационной безопасности в организации. Предполагается, что читателем движет желание применить свои знания по информационной безопасности для улучшения планирования, выполнения и поддержания информационной безопасности и добиться высокоэффективной программы информационной безопасности, которая могла бы быть сертифицирована по стандарту ISO 27001. Эта глава начинает обсуждение с обзора стандартов по безопасности и уделяет особое внимание существующим и разрабатываемым стандартам Международной Организации по Стандартизации (International Standards Organization - ISO).

1.1 Цели

Эта глава посвящена следующему:

- Краеугольные камни информационной безопасности
- Краткая история стандартов ISO по безопасности
- Перечень стандартов ISO по безопасности и назначение каждого из них
- Введение в стандарты ISO 27001 и 27002
- Связи между стандартам ISO 27001 и ISO 27002
- Связи между стандартам ISO 27001 и 27002 и другими стандартами ISO на системы менеджмента
- Знакомство с моделью Plan-Do-Check-Act (PDCA).

Этот материал дает основы для понимания систем менеджмента информационной безопасности (СМИБ), без которых невозможно обеспечить сертификацию по ISO 27001.

1.2 Краеугольные камни информационной безопасности

Традиционные активы организации, как правило, имеют материальную форму, выступая в виде собственности, оборудования, зданий, рабочих мест, денежных средств или иных оборотных средств, например, золота. Заботы о безопасности ранее понимались более в физическом смысле, находя свое выражение в охране, стенах, хранилищах и сейфах. Сегодня же активы организации имеют, кроме этого, и виртуальные активы, такие как интеллектуальную собственность, размещенную на электронных носителях (например, текстовые файлы, электронные таблицы и базы данных). Более того, оборотные активы представляются битами на жестком диске и транзакциями, выполняемыми путем передачи единиц информации по сетям, проводным или беспроводным. Достояние организации в значительной степени представлено битами информации, поэтому существует необходимость защитить эти активы посредством механизмов управления информационной безопасностью. Традиционный взгляд на информационную безопасность включает три «краеугольных камня»: конфиденциальность, целостность и доступность, известные также как «модель CIA (Confidentiality-Integrity-Availability). Конфиденциальность, целостность и доступность являются целями безопасности, при том, что назначение конфиденциальности состоит в том, чтобы гарантировать, что только имеющий соответствующие полномочия персонал может получит доступ к информации или, наоборот, гарантировать, что информация не будет раскрыта не уполномоченным лицам или иным объектам (например, автоматизированной системе или службе). Сохранять целостность означает обеспечивать защиту от несанкционированного изменения или повреждения информации, или обеспечивать сохранение информации в той форме, которую предполагал ее создатель. Потеря целостности означает несанкционированное изменение или повреждение информации. Доступность означает, что информация может быть использована, когда это необходимо. Потеря доступности выражается в нарушении либо доступа к информации, либо возможности ее использования, либо информационной технологии. Рисунок 1.1. показывает эти три «краеугольных камня» конфиденциальности, целостности и доступности (CIA). FIPS PUB 199 содержит больше деталей по этим трем составляющим.

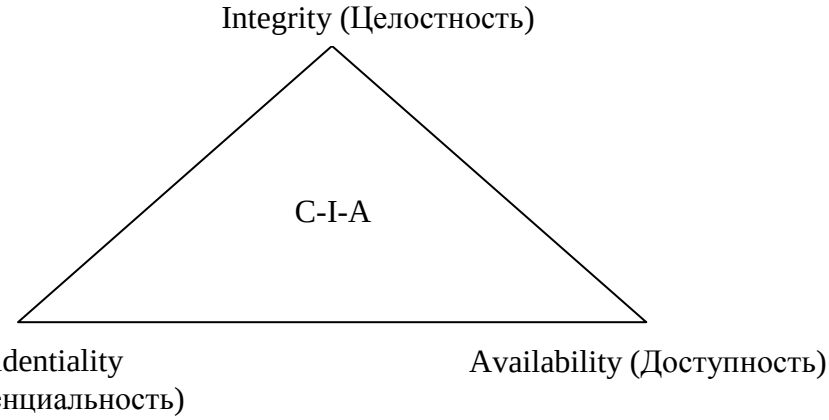


Рис. 1.1 Краеугольные камни безопасности

Как может организация управлять информационной безопасностью и этими тремя компонентами? Один ответ состоит в том, чтобы внедрить Систему Менеджмента Информационной Безопасности (СМИБ, ISMS) и использовать стандарты ISO как руководство по разработке результативной системы. Модель PDCA дает методологию внедрения СМИБ. Стандарта ISO 27002 (бывший стандарт ISO 17999) обеспечивает базис для результативной СМИБ, а ISO 27001 – руководство по тому, как внедрить СМИБ посредством процессов, выстроенных по модели PDCA.

1.3 История стандартов ISO по информационной безопасности

Министерство торговли и промышленности Великобритании (DTI) сформировало рабочую группу для разработки свода лучших практик по обеспечению безопасности. DTI опубликовало в 1989 году стандарт[4] под названием *User Code of Practice.* Этот стандарт представлял собой перечень средств управления безопасностью, которые, на то время, представлялись подходящими, нормальными и хорошими, применимыми как к технологии, так и среде того времени.

Рисунок 1.2 показывает историю разработки стандартов ISO 27001[1] и ISO 17999[2] (ISO 27002). Документ DTI был опубликован как руководящий документ британской системы стандартов (BS), а позже – как британский стандарт BS 7799:1995, Part 1. Первая часть включала в себя перечень средств управления, которые представляли собой набор лучших практик в области обеспечения информационной безопасности. Вторая часть стандарта была выпущена под названием BS 7799:1998, Part 2. Она представляла собой инструменты для измерения и мониторинга в рамках средств управления, описанных в Part 1, а также давала возможность бенчмаркинга при ориентации на сертификацию. В ходе последовательных пересмотров первая часть была опубликована как BS 7799:1999, Part 1, предложена ISO и выпущена как стандарт ISO 17999:2000. Новая версия второй части была выпущена как BS 7799:2002, Part 2. Стандарт ISO 17999 был вновь пересмотрен и выпущен как ISO 17999:2005, а потом ему изменили название на

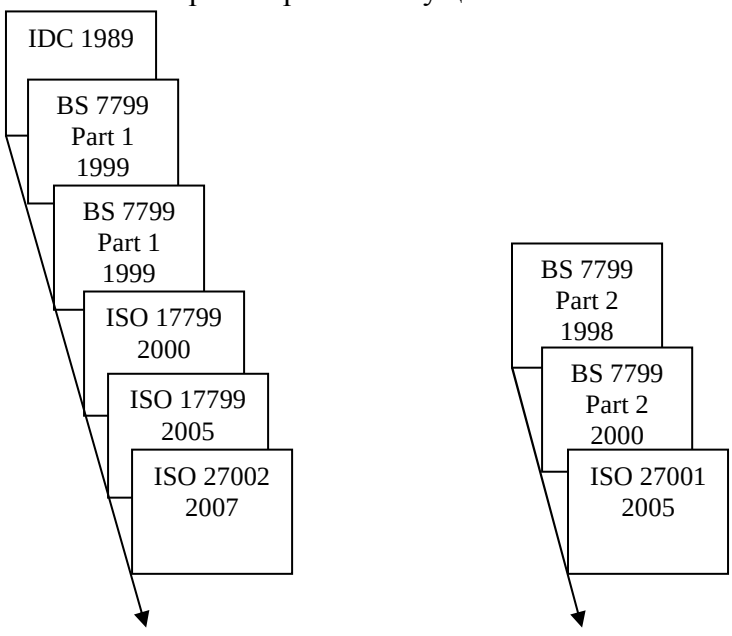


Рис. 1.2 Развитие стандартов ISO 27001 и 27002

ISO 27002:2005. В июле 2007 года стандарт BS 7799, Part 2 был предложен ISO и выпущен этой организацией как стандарт ISO 27001:2005. в следующем разделе рассказывается о том, как сформировалась серия стандартов ISO 27000.

1.4 Формирование и нумерация стандартов по информационной безопасности

ISO и Международная Электротехническая Комиссия (МЭК, IEC) разрабатывают совместно международные стандарты и руководства. Одна из общих целей – выпуск стандартов по менеджменту безопасности. В коллективную работу по формированию стандартов включены Рабочая группа 1 (WG1), Рабочая группа 2 (WG2) и Рабочая группа 3 (WG3). Все эти рабочие группы являются частью Подкомитета 27 (SC 27), который, в свою очередь, входит в Совместный Технический Комитет 1 (JTC 1)[5]. Областью назначения Рабочей группы 1 является разработка стандартов управления безопасностью, включая вопросы, относящиеся к новым разработкам стандартов по информационной безопасности и разработке стандартов на СМИБ. Цель WG 1 – обеспечить ориентиры, которые бы указали требования к будущему набору международных стандартов и руководств для определения, внедрения, эксплуатации, мониторинга и поддержки СМИБ. Чтобы поддержать такой план развития ISO/IEC решили изменить нумерацию для международных стандартов по информационной безопасности на новую – 27000.

1.5 Международные стандарты управления безопасностью

Таблица 1.1 представляет список и короткое описание некоторых стандартов по безопасности, которые были опубликованы в рамках серии 27000. Любой документ, помеченный как «в разработке» является лишь предполагаемым на момент написания этой книги.

Таблица 1.1 Семейство стандартов ISO 27000

Стандарт ISO/IEC	Описание
Словарь и определения (В разработке)	
27001	Требования к системе менеджмента информационной безопасности (спецификация)
27002	Свод практик по обеспечению информационной безопасности, менеджмент
27003	Руководство по внедрению (В разработке)
27004	Система показателей и измерение (В разработке)
27005	Менеджмент рисков (В разработке)

Стандарт ISO 27001 детально обсуждается в этой книге и он является новым международным стандартом по безопасности, основанным на BS 7799, Part 2. Организации, уже сертифицированные по BS 7799, Part 2 будут вынуждены обновить свои сертификаты в соответствии с последней версией стандарта ISO 27001. ISO 27002 – это просто новое название стандарта ISO 17799. ISO/IEC 27003 содержит руководство по внедрению и базируется на приложении В стандарта BS 7799, Part 2; дата публикации этого стандарта еще ожидается. Модель PDCA, также описываемая в BS 7799, Part 2 (и ISO 27001), не только применяется при внедрении стандартов по информационной безопасности, но и широко применяется в других стандартах по менеджменту, включая ISO 9001 и ISO 14001. ISO 27004 будет определять, как сформировать систему показателей для измерения результативности СМИБ; и также дата выхода стандарта только ожидается. ISO 27005 будет, вероятно, посвящен риск-менеджменту и будет сравним с BS 7799, Part 3 *Guideline for Information Security Risk Management.* Другие планируемые в настоящий момент стандарты серии 27000 – это ISO 27006, который, возможно, будет представлять собой руководство по процессу сертификации/регистрации, и ISO 27007 – Руководство по аудиту СМИБ.

1.6 Другие предложенные стандарты по информационной безопасности

ISO рассматривает ряд других стандартов, все из которых будут частью запланированных мероприятий по созданию серии международных стандартов по управлению информационной безопасностью, включая стандарты, определяющие:

- Рекомендации по мониторингу и пересмотру СМИБ
- Внутренним аудитам СМИБ
- Непрерывному улучшению СМИБ.

Другие предлагаемые стандарты ориентированы на специфические отрасли, такие как здравоохранение, телекоммуникации, финансы и страхование. Полагая, что безопасность – это не цель, а процесс, разработка и развитие стандартов будут постоянными. Как было отмечено ранее, эта книга посвящена стандартам ISO и только для стандартов от ISO/IEC дана перспектива на ближайшее будущее. Однако другие национальные и международные органы имеют стандарты, которые могут помочь определить, внедрить, эксплуатировать, вести мониторинг и поддерживать результативную СМИБ. Сюда можно отнести, но не ограничивая этим, Национальный институт стандартов и технологии (NIST), равно как и множество стандартов, посвященных защите, из США и других стран мира.

1.7 Введение в стандарт ISO 27001

ISO 27001 описывает общую модель внедрения и функционирования СМИБ, а также действий по мониторингу и улучшению системы. ISO следует намерению гармонизировать различные стандарты на системы менеджмента, такие как ISO/IEC 9001:2000, который посвящен менеджменту качества, и ISO/IEC 14001:2004, предназначенный для систем экологического менеджмента. Цель ISO состоит в том, чтобы обеспечить единство и целостность внедрения и функционирования СМИБ с другими системами менеджмента в организации. Сходство стандартов отражает сходство в инструментарии и функциях для внедрения, управления, пересмотра, проверки и сертификации. Это подразумевает, что, если организация внедрила принципы менеджмента одного стандарта, то может быть один аудит и одна система менеджмента, в которой одни и те же принципы применены к менеджменту качества, экологическому менеджменту, менеджменту безопасности и т.д.

Стандарт ISO 27001 содержит руководство как по внедрению СМИБ, так и по получению сертификата третьей стороны, свидетельствующего, что средства управления безопасности существуют и функционируют в соответствии с требованиями этого стандарта. Стандарт ISO 27001 описывает СМИБ как всеохватывающую систему менеджмента, построенную на принципах бизнес-рисков, для внедрения, эксплуатации, мониторинга и поддержки системы управления безопасностью. СМИБ должна охватывать все аспекты организационной структуры, политик, планируемых действий, ответственностей, практик, процедур, процессов и ресурсов. Этот текст является дополнительным к стандарту и не заменяет его; авторы рекомендуют иметь стандарты ISO, имеющие ценность с точки зрения текущих целей организации, чтобы иметь полный набор необходимых документов.

Имея соответствующую СМИБ, высшее руководство обладает средствами мониторинга и контроля безопасности, что уменьшает остаточный бизнес-риск. После внедрения СМИБ организация может официально сохранять информацию и продолжать выполнять требования клиентов, акционеров, а также законодательные и иные обязательные требования. Если целью является сертификация, проанализируйте положения разделов 4 – 8 стандарта ISO 27001, так как эти разделы являются обязательными для сертификации. Приложение А содержит перечень объектов контроля и средств управления, которые совпадают со средствами управления в ISO 27002, но не столь детализированы. Приложение В содержит таблицу, в показано, как соответствующие процедуры СМИБ и фазы PDCA соотносятся с принципами Организации по экономическому сотрудничеству и развитию (OECD). Если организация уже внедрила ISO 9001 или ISO 14001, то приложение С содержит таблицу, показывающую взаимосвязь требований стандартов ISO 9001, 14001 и 27001.

Рисунок 1.3 отображает модель PDCA, используемую для внедрения СМИБ; эта модель иногда обозначается как «цикл СМИБ». Используйте эту модель для разработки, поддержания и постоянного улучшения СМИБ. Целью внедрения СМИБ является построение всеобщей системы менеджмента, разработанной с учетом бизнес-рисков, для того, чтобы внедрить, управлять, вести мониторинг, поддерживать и улучшать защиту информации. Разделы с 4 по 8 стандарта ISO 27001 являются обязательными для прочтения, т.к. они описывают, как организация должна построить и внедрить свою СМИБ.в этих разделах содержатся основные требования к СМИБ, включая те, что определяют как определять систему, управлять ею, вести мониторинг и поддерживать.

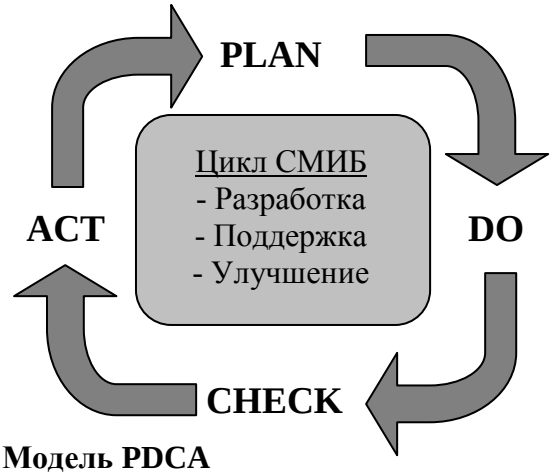


Рис. 1.3 Модель PDCA

1.8 Введение в стандарт ISO 27002

Стандарт ISO 27002 *Code of Practice for Information Security* (Свод практик по информационной безопасности) является международным стандартом общего применения и обеспечивает понимание средств управления, обеспечивающих защиту информации и информационных технологий. ISO 27002 не определяет, как применять эти средства управления. Он обеспечивает руководство по тому, как установить систему менеджмента, которая определяет, как выбрать средства управления и адаптировать хорошие практики, чтобы применить средства защиты. Выбор процедур для фактического внедрения средств защиты остается за организацией и он будет зависеть от физического или технического окружения.

Что такое информационная безопасность и почему она важна? Информационная безопасность – это защита активов организации (например, информации) от неавторизованного раскрытия или неавторизованного или случайного изменения, а также гарантия того, что информация готова к использованию в тот момент, когда она нужна. Законодательство и другие совместимые требования говорят о секретности и точности финансовых отчетов (например, закон Сарбейнса-Оксли) и, обычно, включают потребность в средствах управления защитой в отношении информации. Традиционно активы организации понимаются как материальные активы, подобно оборудованию или зданиям, или оборотные активы, как, например, акции, бонды, валюта или золото. Традиционная стоимость организации также включает в себя нематериальные показатели вроде репутации и относительно меньшее значение придавалось таким ценностям как знания, интеллектуальная собственность или информация. Возрастание зависимости организации от информации, ценность информации для организации и ценность организации, которая владеет информацией (например, интеллектуальной собственностью) находит свое отражение в необходимости защищать эту информацию. Более того, угрозы, связанные с прежним пониманием активов, были ограничены физическим контактом, например, требовался доступ к золоту, чтобы украсть его. К тому же вор нуждался в транспортировке золота из хранилища по зданию, он должен был миновать охрану и, скрываясь, ему необходимо было пересечь штат, страну и национальные границы.

Информационные активы хранятся постоянно доступными в виде документов, баз данных или иных формах хранения информации. Доступ к информационным активам организации посредством множества путей, включая использование компьютеров сотрудников и внутренних сетей. Если организация связана с партнерами, их сети, в целом, представляют собой еще множество потенциальных путей доступа. Если организация подключена к Интернету, она доступна, практически, всему миру. Возможность получения информации в средней части штата Миссури США столь же легка, как и с компьютера в Малайзии. Доступность и простота передачи данных делают бессмысленными все ограничения, связанные с материальными активами.

При этом кража и использование интеллектуальной собственности может быть в стране, которая не признает такие действия незаконными и, если это так, то эта страна может и не иметь соглашений о выдаче преступников с США, Великобританией, Исландией или другими странами. Более того, подобные кражи могут поощряться государством, чтобы обеспечить конкурентоспособность страны на мировом рынке. Проблема в том, что существует широкое разнообразие мотивов, средств и методов, которые делают возможными кражи информационных

активов организации. Таким образом, чтобы оставаться жизнеспособной, организация должна отнестись серьезно к защите информации и внедрить СМИБ, используя описанные подходы. Чтобы обеспечить результативность СМИБ, организация может выбрать в качестве модели стандарты ISO. ISO 27002 включает в себя 12 глав, посвященных средствам управления:

- Оценка и снижение риска
- Политика безопасности
- Организация информационной безопасности
- Управление активами
- Безопасность персонала
- Управление коммуникациями и операциями
- Контроль доступа
- Формирование требований к информационной системе, ее разработка и поддержка
- Управление инцидентами в области защиты информации
- Управление непрерывностью бизнеса
- Соответствие

Эти 12 глав описывают примерно 39 ключевых элементов и 133 механизма управления. Таблица 1.2 иллюстрирует структуру и содержание каждой части описания механизма управления.

Таблица 1.2 ISO 27002 – структура описания механизма управления безопасностью

Управление (Control)	Определение методов управления безопасностью с установлением свойств, необходимых для удовлетворения требований к управлению
Руководство по внедрению (Implementation guidance)	Включает информацию для внедрения средств управления и рекомендации по удовлетворению требований к средствам управления
Другая информация	Описание некоторых механизмов контроля содержит раздел «Другая информация», где указаны ссылки на информацию, связанную с этим механизмом контроля

Используйте эти рекомендации при написании политик и процедур, а также определения назначения на основании целей разделов. Затем используйте разъяснения для каждого механизма контроля, чтобы детализировать политики и процедуры соответственно назначению.

1.9 Взаимосвязь ISO 27001 и 27002

Стандарт ISO 27001 представляет систему менеджмента для обеспечения информационной безопасности. ISO 27002 содержит рекомендации по механизмам управления безопасностью. . ISO 27002 – это больше «*что*» (т.е., перечень полезных средств управления), а ISO 27001 – больше «*как*» (т.е. процедура того, как настроить систему менеджмента, описывающая, как создать и поддерживать механизмы управления). ISO 27001 – это не набор процедур, которые раскрывают каждый механизм управления из ISO 27002; скорее, это процесс управления, чтобы обеспечить понимание безопасности, организационную инфраструктуру, а также спланировать, внедрить и поддерживать механизмы управления безопасностью. Организация может не получать сертификат на соответствие ISO 27002, она получает сертификат на систему менеджмента информационной безопасности, требования к которой установлены в ISO 27001.

Приложение А стандарта ISO 27001 перечисляет механизмы управления, данные в ISO 27002, в точно том же порядке; однако дается только короткое описание этих средств управления, содержащееся в ISO 27001. Оба стандарта вместе с рекомендациями этой книги обеспечивают возможность сертификации на соответствие ISO 27001.

1.10 Взаимосвязь с другими стандартами

ISO разрабатывает разные стандарты для систем менеджмента; ISO 9000 – для менеджмента качества, ISO 14000 – для экологического менеджмента и ISO 27000 - для менеджмента безопасности. ISO 27001 содержит описание взаимосвязи СМИБ с другими стандартами на системы менеджмента. ISO 27001 направлен на гармонизацию с другими стандартами на системы менеджмента, чтобы обеспечить единое и цельное внедрение и функционирование системы

менеджмента предприятия. Стандарты по информационной безопасности используют модель PDCA для внедрения, мониторинга и улучшения СМИБ. Другие стандарты также используют эту модель. Общее между всеми этими стандартами заключается в следующем:

- Все предполагают обязательства менеджмента
- Определение ответственности
- Управление документами
- Обучение
- Анализ системы руководством
- Внутренние аудиты
- Корректирующие и предупреждающие действия
- Общая модель PDCA для внедрения и функционирования
- Процессы аудита
- Схема оценки уполномоченными лицами, основанная на требованиях международного стандарта ISO 19011:2002 Guidelines on Quality and/or Environmental Management System Audit16
- Требования, изложенные в схожих стандартах
- Орган по сертификации ответственен за проверку компетенции аудитора.

Если есть возможность, организации, намеревающиеся внедрить и использовать несколько стандартов на системы менеджмента, могут расширить свою СМИБ, с тем, чтобы распространить ее на все другие системы менеджмента. Такое использование СМИБ может быть названо Программой по совмещению систем менеджмента (Compliance Management Program – CMP) [см. главу 6]. Выгоды от единой системы менеджмента заключаются во вложениях только на одну систему менеджмента, в едином аудите и единой сертификации, что снижает затраты организации.

1.11 PDCA и стандарты безопасности

Любой перечень лучших практик, содержащийся в международных, национальных или иных стандартах, будет неполным. Тем не менее этот раздел представляет некоторые из наиболее общих стандартов, связанных с моделью PDCA (числа в скобках являются ссылками на элементы списка, приведенного в конце книги).

1.11.1 Стандарты, полезные на фазе планирования (PLAN)

ISO/IEC 27001, Information Technology — Security Techniques — Information Security Management Systems — Requirements, Первая редакция, действует с 15 октября, 2005 г, доступен на сайте www.iso.org.

Control Objectives for Information and Related Technology (COBIT), доступен на сайте www.isaca.org.

ISO/IEC 17799, Information Technology — Security Technique s— Code of Practice for Information Security Management, вторая редакция, действует с 15 июня 2005 г, доступен на сайте www.iso.org (сейчас это стандарт ISO 27002).

FIPS PUB 199, Federal Information Processing Standards Publication — Standard for Federal Information and Information Systems, редакция от февраля 2004 г, доступен на сайте www.nist.gov.

SP 800-60, Guide to Mapping Types of Information Systems to Security Categories, доступен на сайте www.nist.gov.

SP 800-30, Risk Management Guide for Information Technology Systems from NIST [National Institute of Standards and Technology], доступен на сайте www.nist.gov.

ISO TR 13335-4:2000. Covers the selection of safeguards (meaning technical security controls). Этот стандарт в настоящее время пересматривается и будет выпущен как ISO 27005, доступен на сайте www.iso.org.

SP 800-18, Guide for Developing Security Plans for Information Technology Systems, доступен на сайте www.nist.gov. Руководство по разработке и документированию средств управления безопасностью в ИТ.

SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, проект доступен на сайте www.nist.gov.

BS 7799-3:2006, Guidelines for Information Security Risk Management, доступен на сайте http://www.bsonline.bsi-global.com/server/index.jsp.

ISO/IEC TR 13335-3, Guidelines for the Management of IT Security: Techniques for the Management of IT Security from International Organization for Standardization, доступен на сайте www.iso.org.

1.11.2 Стандарты, полезные на фазе выполнения (DO)

ISO/IEC 27001, Information Technology — Security Techniques — Information Security Management Systems — Requirements, Первая редакция, действует с 15 октября, 2005 г, доступен на сайте www.iso.org.

ISO/IEC 17799, Information Technology — Security Technique s— Code of Practice for Information Security Management, вторая редакция, действует с 15 июня 2005 г, доступен на сайте www.iso.org (сейчас это стандарт ISO 27002).

SP 800-53, Recommended Security Controls for Federal Information Systems, доступен на сайте www.nist.gov. Фактически, другой стандарт на СМИБ, содержащий удобную таблицу, показывающую связь средств контроля, описанных в нем, со средствами контроля, задаваемыми в других стандартах, таких, как ISO 17799:2005.

SP 800-55 [в книге ошибочно указано SP 800-5 – прим. перев.], Security Metrics Guide for Information Technology Systems, доступен на сайте www.nist.gov. Название, на мой взгляд, гораздо привлекательнее содержания. Документ, по сути, немногим более, чем просто огромный список параметров, относящихся к безопасности, и которые могут быть измерены.

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, доступен на сайте www.nist.gov.

ISO TR 13335-4:2000. Covers the selection of safeguards (meaning technical security controls). Этот стандарт в настоящее время пересматривается и будет выпущен как ISO 27005, доступен на сайте www.iso.org.

1.11.3 Стандарты, полезные на фазе проверки (CHECK)

SP 800-61, Computer Security Incident Handling Guide, доступен на сайте www. nist.gov.

SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, available from www.nist.gov. Содержит руководство по сертификации защиты, аккредитации и авторизации информационных систем

SP 800-53, Recommended Security Controls for Federal Information Systems, доступен на сайте www.nist.gov. Фактически, другой стандарт на СМИБ, содержащий удобную таблицу, показывающую связь средств контроля, описанных в нем, со средствами контроля, задаваемыми в других стандартах, таких, как ISO 17799:2005.

SP800-26, Government Audit Office Federal Information System Controls Audit Manual, доступен на сайте www.nist.gov.

1.11.4 Стандарты, полезные на фазе улучшения (ACT)

ISO/IEC 27001, Information Technology — Security Techniques — Information Security Management Systems — Requirements, Первая редакция, действует с 15 октября, 2005 г, доступен на сайте www.iso.org.

ISO/IEC 17799, Information Technology — Security Technique s— Code of Practice for Information Security Management, вторая редакция, действует с 15 июня 2005 г, доступен на сайте www.iso.org (сейчас это стандарт ISO 27002).

SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, available from www.nist.gov. Содержит руководство по сертификации защиты, аккредитации и авторизации информационных систем

ISO 19011:2002, Guideline on Quality and/or Environmental Management System Audit, доступен на сайте www.iso.org. Схема оценки уполномоченными лицами, базирующаяся на общем международном стандарте

Глава 2 Система менеджмента информационной безопасности

В предыдущей главе рассказывалось о стандартах ISO по безопасности, текущем состоянии, планах на будущее и взаимосвязи стандартов ISO друг с другом. ISO 27001 служит руководством по созданию системы менеджмента информационной безопасности (СМИБ) и ссылается на средства управления, описанные в ISO 27002, которые позволяют внедрить и поддерживать

СМИБ. Эта глава определяет и представляет СМИБ как необходимое условие для обсуждения основных концепций и инструментов, необходимых для результативного построения СМИБ.

2.1 Цели

Цели этой главы:

- Определить СМИБ
- Пояснить, что имеет в виду ISO, используя термин «СМИБ»
- Вкратце определить факторы, побуждающие бизнес к построению СМИБ
- Представить концепции СМИБ, существующие вне рамок ISO, и показать их перспективы:
  - Общая схема менеджмента безопасности (Security management framework)
  - «Как должно быть» (To-be)
  - «Как есть» (As-is)
  - Анализ упущений (Gap analysis)
  - План перехода
- Обеспечить понимание общих терминов до их применения в контексте основных идей и механизмов, которые обеспечивают функционирование СМИБ

2.2 Представление СМИБ

ISO определяет СМИБ как «часть общей системы менеджмента, базирующаяся на оценке бизнес-рисков, необходимая для создания, внедрения, функционирования, мониторинга, пересмотра, поддержки и улучшения информационной безопасности»[*]. В соответствии с определением ISO «общая система менеджмента» в организации включает в себя много больше, чем только безопасность и, на самом деле, ISO предлагает несколько стандартов, относящихся к системам менеджмента. Семейство ISO 9000 представляет собой серию стандартов, связанных с системами менеджмента качества. Семейство ISO 14000 является набором стандартов по систем экологического менеджмента. ISO 27000 – это семейство стандартов на системы менеджмента безопасности. Поэтому ISO вводит термины, которые могут быть применимы ко всем системам менеджмента, и использует их, чтобы определить действия, необходимые для создания, поддержания и улучшения менеджмента информационной безопасности.

Есть и другие названия для СМИБ: *программа управления безопасностью* (Security Management Program – SMP), *программа страхования информации* (Information Assurance Program – IAP) и много других возможных. Термины SMP и IAP встречались в практике автора, но не используются ISO. Эти термины упомянуты для того, чтобы сделать более ясным смысл понятия *система менеджмента информационной безопасности*. Дело в том, что многие могут придти в замешательство, пытаясь понять применение ISO термина *система*. ISO под этим словом в СМИБ понимает процесс или методологию. Многие же будут понимать под системой действующее устройство или приложение. Держа в уме сертификацию по ISO 27001, используйте термин *СМИБ* в том смысле, в каком его использует ISO, или используйте другие термины, но точно убедившись, что они имеют тот же смысл. В дальнейшем в тексте термин *СМИБ* будет использоваться в том значении, которое предлагает ISO; если случайно встретите термин *программа безопасности* (*security program*) просто замените на *СМИБ* - они в этой книге равнозначны.

2.3 Знакомство с общей схемой менеджмента безопасности

Используете ли вы термин СМИБ или какой-то другой, процесс, инструментарий, шаблоны, документы и практики для достижения результативности СМИБ одни и те же. Полагая справедливым, что принцип «один размер на всех» не работает, необходимо адаптировать программу по безопасности или СМИБ к особенностям организации. И правильно будет начать это с разработки ориентированной на конкретную организацию общей схемы менеджмента безопасности (Security Management Framework – SMF).

SMF задает контуры для определения, обсуждения, планирования, внедрения, отслеживания и отчетности по проблемам безопасности, важным для организации. Хорошая SMF базируется на

[*] ISO/IEC 27001:2005, *Information Security Management Systems—Requirements*, p. 2.

отраслевом стандарте для обеспечения полноты и целостности и, как правило, предполагает применение лучших отраслевых практик. Организация может как добавлять что-то к положениям стандарта, так и убирать, чтобы определить SMF в соответствии с потребностями организации. Есть немало стандартов, из которых можно выбрать. Краткий перечень стандартов по безопасности включает стандарты ISO, Национального Института Стандартов и Технологий (National Institute of Standards and Technology – NIST), Специальные Публикации (Special Publications – SP), Федеральные Стандарты Обработки Информации (Federal Information Processing Standards - FIPS), серию стандартов 8500.x Министерства Обороны США, включая Руководство по техническому обеспечению безопасности (Security Technical Implementation Guide – STIG), Европейской сети и агентства по информационной безопасности (European Network and Information Security Agency – ENISA) и многих других.

В этой книге упор сделан на стандарты ISO, как на совокупность международных стандартов, применимых к коммерческим организациям. Разработка SMF может учитывать также многие другие совместимые требования, например, закона Сарбейнса-Оксли (США) или Health Insurance Portability and Accountability Act (HIPAA). Многие требования в иных совместимых документах будут пересекаться с требованиями стандартов ISO. По этой причине SMF, базирующаяся на стандартах ISO, удовлетворит – по умолчанию – во всяком случае, ряд других совместимых требований. Например, создание рабочей группы по безопасности (Security Working Group - SWG) с участием представителей, выполняющих различные функции в организации, соответствует требованию ISO 27001. И это же удовлетворяет требование HIPAA. Построение одной SMF с возможностью проследить выполнение различных совместимых требований дает возможность удовлетворить многие требования за один раз. Об этой возможности мы поговорим в следующих разделах.

2.4 Процесс построения СМИБ: «Как должно быть» (To-be) или цикл PDCA

Приверженцы подходов ISO используют для построения СМИБ модель Plan-Do-Check-Act (PDCA). ISO применяет эту модель во многих своих стандартах по менеджменту и ISO 27001 не исключение. Более того, следование модели PDCA в практике менеджмента обеспечивает возможность использовать те же приемы и для менеджмента качества, экологического менеджмента, менеджмента безопасности, а также в других сферах менеджмента, снижая затраты. Вследствие этого PDCA – это замечательный вариант и отвечает рассматриваемым задачам по построению и поддержанию СМИБ. Иными словами, фазы PDCA определяют, как установить политику, цели, процессы и процедуры, существенные с точки зрения менеджмента рисков (фаза планирования - Plan), внедрить и использовать (фаза выполнения – Do), оценивать и, там где это возможно, измерять результаты процесса с точки зрения политики (фаза проверки – Check) и выполнять корректирующие и предупреждающие действия (фаза улучшения – Act). В дополнении к этому могут быть указаны иные (не ISO) концепции, которые могут быть полезными при построении СМИБ:

- Определение состояния «Как должно быть»
- Определение состояния «Как есть»
- План перехода

В контексте управления бизнес-рисками состояние «Как должно быть» определяет желаемое состояние. Оно включает в себя вовлечение менеджмента, организационные структуры, область действия, политики, стандарты, процедуры и многое другое. Комбинация ISO 27001 и ISO 27002 устанавливает соответствующее состояние «Как должно быть» для многих организаций, то есть подход организации к безопасности должен соответствовать системе менеджмента и средствам управления, определяемым этими стандартами. Разработку SMF можно начать с ISO 27002, добавляя требования других стандартов, чтобы создать SMF, отвечающую потребностям организации; эта SMF затем станет основой состояния «Как должно быть» для конкретной организации.

В контексте менеджмента рисков состояние «Как есть» это некий фотоснимок текущего состояния с безопасностью. Для получения такого «снимка» используется набор инструментов, основанных на SMF. Сравнение состояний «Как есть» и «Как должно быть» - это и есть анализ упущений (Gap-анализ). Процесс такого анализа и отчеты о нем также основываются на SMF.

Следующий раздел конкретизирует вопросы, связанные с состояние «Как должно быть», «Как есть» и планом перехода в контексте СМИБ и управления бизнес-рисками.

Попутное, но весьма важное замечание. Использование до этого момента в книге терминов «Как должно быть» (To-be), «Как есть» (As-is) и «план перехода» служило цели познакомить читателей с этими понятиями. Повторю, ISO эти термины не применяет. Последняя часть книги представляет подробно *compliance management*[*] и состояния «Как должно быть», «Как есть» и план перехода являются составными частями абстрактного подхода к оценке соответствия (это часть *compliance management*). Как будет детально показано в главе 6 «Compliance management» создание и поддержание СМИБ – это пример более абстрактного процесса *compliance management*'а. Основное назначение этой книги – знакомство с применением и приложением стандартов ISO по безопасности и получение сертификата соответствия по ISO 27001. Второе – но крайне важное – назначение этой книги состоит в том, чтобы познакомить со всеми проявлениями *compliance management*'а, среди которых получение сертификата по ISO 27001 – всего лишь один аспект. Комбинируя эти концепции с учетом их взаимосвязей, читатель сам будет способен создать инструменты *compliance management*'а, которые, будучи использованы для сертификации по ISO 27001, могут быть использованы для создания других систем, основанных на бизнес-рисках, тем самым снижая расходы.

2.4.1 Установить «Как должно быть» (To-be)

Эта стадия определяет объекты защиты в терминах управления рисками и очерчивает границы, в рамках которых будет выстраиваться СМИБ. Объекты, связанные с бизнесом, определяют содержание СМИБ. Для сертификации по ISO 27000 необходимо выполнить требования, содержащиеся с разделах 4-8 стандарта ISO 27001. Определение общей схемы системы (Security Management Framework, SMF) позволяет определить и СМИБ. Глава 3 «Основные концепции и инструменты для СМИБ» конкретизирует вопросы, связанные с SMF.

На стадии определения состояния «Как должно быть» мы получаем общую схему системы, учитывающую все особенности конкретной организации, и содержащую перечень требований по безопасности, которые основываются на отраслевых стандартах и которые привязаны к бизнес-рискам этой организации. Первое, для чего используется эта общая схема, это определение интерпретации руководящих указаний с тем, чтобы создать общий перечень терминов и их определений, а также обеспечить единое понимание концепций, необходимых для поддержки СМИБ.

Определение состояния «Как должно быть» относиться к фазе планирования (Plan) модели PDCA. Помните, что в данном случае фаза планирования служит для определения объектов, в отношении которых разрабатывается СМИБ. На этой стадии преждевременно разрабатывать политику или процедуры; эти действия уместны на стадии выполнения (Do) или как часть плана перехода, который описывает мероприятия, по переходу от состояния «Как есть» к состоянию «Как должно быть».

2.4.2 Установить состояние «Как есть»

На этом шаге определяется текущее состояние организации в области управления безопасностью для сравнения с системой, определенной на стадии разработки состояния «Как должно быть». Установление состояния «Как есть» включается в себя процессы исследования, анализа (gap-анализ) и отчета о результатах. Глава 3 подробно рассказывает об этом и в ней также даются различные шаблоны (в том числе и вопросников для стадии исследования).

На данном этапе разрабатывают опросный лист, отражающий специфику общей схемы системы (SMF). Кроме этого создаются краткое описание проекта, шаблоны для записи результатов, аналитические инструменты для изучения результатов и формирования полезных предложений, и, в конечном итоге, отчет, который показывает текущее состояние («снимок») организации в области менеджмента безопасности. Термин «снимок» указывает на то, что состояние с управлением безопасностью динамично и может быстро меняться; таким образом,

---

[*] Compliance management – менеджмент, основанный на соблюдении требований внешних и внутренних нормативных документов. Например, менеджмент качества в соответствии с требованиями ISO 9001. К сожалению, адекватного перевода термина на русский язык пока не существует. Compliance management можно определить как «Менеджмент на основе соответствия». [прим. перевод.]

любые результаты изучения текущего состояния привязаны ко времени и имеют ограниченное время актуальности, в течение которого организация может их использовать для принятия соответствующих решений.

Деятельность по установлению состояния «Как есть» относится к фазам планирования и проверки модели PDCA: начальное планирование СМИБ – к фазе планирования, а непрерывное отслеживание и пересмотр – к фазе проверки. Существует возможность использовать одни и те же инструменты на обеих фазах. Более того, мотивом к этому служит возможность облегченного сравнения результатов, полученных на стадии начального планирования и постоянного анализа действий.

2.4.2 План перехода

План перехода содержит конкретные шаги по изменению состояния «Как есть» в состояние «Как должно быть». Этот процесс может потребовать более одного бюджетного цикла, в зависимости от объема деятельности, необходимой, чтобы СМИБ соответствовала целям. Принимая во внимание продолжительность и возможную высокую стоимость этой деятельности, организация должна установить приоритеты, т.е. соответствующим образом распределить ресурсы, в первую очередь направив их на устранение наиболее существенных для организации рисков. Глава 4 «Внедрение СМИБ – цикл PDCA» подробно рассказывает о разработке плана перехода к СМИБ, удовлетворяющей требованиям ISO 27001.

В ходе разработки плана перехода формируется отчет об анализе необходимых коррекций и документированный план перехода, определяющий хотя бы высший уровень мероприятий. В зависимости от степени детализации, в ходе этой работы могут создаваться требуемым образом оформленное описание целей (т.е. описание проекта), модель затрат с декомпозицией работ, а также план проекта со сроками и результатами работ. План перехода может также предполагать создание соглашений об уровне сервиса (Service Level Agreement – SLA) либо для внешних поставщиков, либо для внутренних исполнителей. Соглашения SLA представляют собой формальный перечень оперативных целей, например, время работоспособности должно составлять не менее 98% от общего рабочего времени.

Создание плана перехода предполагается на фазах выполнения (Do) и улучшения (Act) PDCA-модели. Переход от начального (зафиксированного текущего) состояния осуществляется в фазе выполнения, а постоянный мониторинг и пересмотр, приводящие к формированию измененных планов – в фазе Act.

2.4.4 Стадия эксплуатации

На стадии эксплуатации системы ведется непрерывная поддержка СМИБ, включающая периодические пересмотры целевых состояний («Как должно быть»). Эти пересмотры могут быть вызваны появлением новых стандартов, т.е. изменениями в ISO 27001 или ISO 27002. другими факторами могут быть изменения в законодательстве или иных нормативных документах, изменения в контрактах, а также изменения бизнес-среды, которые приводят к тому, что решаемые задачи перестают соответствовать потребностям.

В ходе эксплуатации производятся измерения и показатели выполнения сравниваются с SLA. Параллельно могут формироваться различного рода отчеты, существенные с точки зрения безопасности, включая журналы (логи), отчеты об инцидентах, поиске основных причин и другие. Эксплуатация системы относится к фазам проверки (Check) и улучшения (Act) модели PDCA.

Ссылки

1. ISO/IEC 27001. Information Technology—Security Techniques—Information Security Management Systems—Requirements, first edition. October 15, 2005. Доступен на сайте www.iso.org.
2. ISO/IEC 17799. Information Technology—Security Techniques—Code of Practice for Information Security Management, second edition. June 15, 2005. Доступен на сайте www.iso.org.
3. FIPS PUB 199. Federal Information Processing Standards Publication—Standard for Federal Information and Information Systems. February 2004. Доступен на сайте www.nist.gov
4. Сайт компании Gamma - http://www.gammassl.co.uk/bs7799/history.html
5. Информация из стандартов ITSC (Standards Technology Standard Committee). Новости о стандартах с форума RAISS. Доступен на сайте http://www.itsc.org.sg/.
6. SP 800-18. *Guide for Developing Security Plans for Information Technology Systems*. Доступен на сайте www.nist.gov. Guides the design and documentation of IT security controls.
7. *OECD Guidance for Security of Information System and Network—Toward a Culture of Security*. Доступен на сайте www.oecd.org. Новые рекомендации OECD от 2002 г. доступны по адресу http://www.oecd.org/dataoecd/16/22/15582260.pdf.
8. Index of the ISO/IEC 17799, second edition. June 15, 2005. From pages III to VI.
9. Shewhart, Walter Andrew (1939). *Statistical Method for the Viewpoint of Quality Control.* New York: Dover. (1980) *Economic Control of quality of manufactured product/ 50th Anniversary Commemorative Issue.* American Society For Quality. Для более детальной иформации:. http:en.wikipedia.org/wiki/Shewhart_cycle.
10. SP 800-60. Guide to Mapping Types of Information Systems to Security Categories. Доступен на сайте www.nist.gov.
11. SP 800-30. Risk Management Guide for Information Technology Systems from NIST [National Institute of Standards and Technology]. Доступен на сайте www.nist.gov.
12. ISO/IEC TR 13335-3. Guidelines for the Management of IT Security: Techniques for the Management of IT Security from International Organization for Standardization. Доступен на сайте www.iso.org.
13. Peltier, T. (2005) Information Security Risk Analysis. Auerbach Publications.
14. Checklist for self-assessment for all controls for BS 7799-2:2002. Доступен по адресу http://www.sans.org/score/checklists/ISO_17799_checklist.pdf. Кроме этого, чек-лист для самооценки от Netigy. Доступен по адресу http://www.cccure.org/modules.php?name= Downloads&d_op=viewdownload&cid=67.
15. Здесь несколько ссылок на пользовательские группы ISMS: U.S. ISMS user group, http://www.us-isms.org/; international user group, http://www.xisec.com/; есть еще информация на ITU в Канаде, http://www.ismsiug.ca; в Японии, www.j-isms.jp.
16. .Схема оценки уполномоченными лицами, базирующаяся на общем международном стандарте — ISO 19011:2002, Guideline on Quality and/or Environmental Management System Audit. Доступен на сайте www.iso.org.
17. Sarbanes–Oxley Act of 2002. Доступен по адресу http://news.findlaw.com/hdocs/docs/ gwbush/sarbanesoxley072302.pdf.
18. Адрес, по которому можно найти информацию по Base II от Европейской Комиссии: http://europa.eu.int/comm/enterprise/entrepreneurship/financing/basel_2.htm.
19. ISO 9001:2000. Quality Management Systems. Доступен на сайте www.iso.org.
20. BS 7799-3:2006. Guidelines for Information Security Risk Management. Доступен по адресу http://www.bsonline.bsi-global.com/server/index.jsp.
21. ISO TR 13335-4:2000 определяет выбор мер безопасности (т.е. технических средств управления безопасностью). Этот стандарт в настоящее время пересматривается и будет выпущен как ISO 27005, доступен на сайте ISO www.iso.org.
22. SP 800-53A. *Guide for Assessing the Security Controls in Federal Information* (draft). Доступен на сайте www.nist.gov.
23. SP 800-53. *Recommended Security Controls for Federal Information Systems*. Доступен на сайте www.nist.gov. Фактически, другой стандарт на СМИБ, содержащий удобную таблицу, показывающую связь средств контроля, описанных в нем, со средствами контроля, задаваемыми в других стандартах, таких, как ISO 17799:2005.
24. SP 800-55. *Security Metrics Guide for Information Technology Systems*. Доступен на сайте www.nist.gov. Название, на мой взгляд, гораздо привлекательнее содержания. Документ, по сути, немногим более, чем просто огромный список параметров, относящихся к безопасности, и которые могут быть измерены.
25. FIPS 200. *Minimum Security Requirements for Federal Information and Information Systems*. Доступен на сайте www.nist.gov.
26. SP 800-61. *Computer Security Incident Handling Guide*. Доступен на сайте www.nist.gov.
27. SP 800-37. *Guide for the Security Certification and Accreditation of Federal Information Systems*. Доступен на сайте www.nist.gov. Содержит руководство по сертификации защиты, аккредитации и авторизации информационных систем.
28. SP800-26. *Government Audit Office Federal Information System Controls Audit Manual*. Доступен на сайте www.nist.gov.
29. SP 800-37. *Guide for the Security Certification and Accreditation of Federal Information Systems*. Доступен на сайте www.nist.gov. Содержит руководство по сертификации защиты, аккредитации и авторизации информационных систем..
30. ISO 19011:2002. *Guidelines for Quality and/or Environmental Management Systems Auditing*. Доступен на сайте www.nist.gov.
31. Control Objectives for Information and Related Technology (COBIT). Доступен на сайте www.isaca.org.
32. Information Technology Infrastructure Library (ITIL). Доступен на сайте www.itsmf.com.