ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27000— 2012

Информационная технология. Методы и средства обеспечения безопасности

СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общий обзор и терминология

ISO/IEC 27000:2009
Information technology — Security techniques — Information security management systems — Overview and vocabulary (IDT)

Издание официальное

Москва
Стандартинформ
2014

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации — «Фирма «ИНТЕРСТАНДАРТ» (ФБУ «КВФ «Интерстандарт») совместно с Евро-Азиатской ассоциацией производителей товаров и услуг в области безопасности (Ассоциация ЕВРААС) и ООО «Научно-испытательный институт систем обеспечения комплексной безопасности» (ООО «НИИ СОКБ») на основе аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 362 «Защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 15 ноября 2012 г. № 813-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27000:2009 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (ISO/IEC 27000:2009 «Information technology — Security techniques — Information security management systems — Overview and vocabulary»).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты Российской Федерации, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (gost.ru)

© Стандартинформ, 2014

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Системы менеджмента информационной безопасности . . . 4
3.1 Основные понятия . . . 4
3.2 Общие положения . . . 4
3.3 Процессный подход для СМИБ . . . 6
3.4 Цели внедрения СМИБ . . . 6
3.5 Внедрение, контроль, поддержка и улучшение СМИБ . . . 7
3.6 Критические факторы успеха СМИБ . . . 8
3.7 Преимущества внедрения стандартов семейства СМИБ . . . 9
4 Семейство стандартов СМИБ . . . 9
4.1 Общая информация . . . 9
4.2 Стандарты, содержащие общий обзор и терминологию . . . 10
4.3 Стандарты, задающие требования . . . 10
4.4 Стандарты, содержащие общие рекомендации . . . 10
4.5 Стандарты, описывающие рекомендации для специальной области . . . 11
Приложение А (справочное) Глагольные формы, используемые для формулировок положений стандартов . . . 12
Приложение В (справочное) Перечень терминов по категориям . . . 13
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 14
Библиография . . . 15

Введение

Международные стандарты системы менеджмента представляют модель для налаживания и функционирования системы менеджмента. Эта модель включает в себя функции, по которым эксперты достигли согласия на основании международного опыта, накопленного в этой области. Подкомитет SC 27 Совместного технического комитета ISO/IEC JTC 1 имеет в своем составе комиссию экспертов, которая работает в области создания системы международных стандартов по информационной безопасности, известной как семейство стандартов системы менеджмента информационной безопасности (СМИБ).

При использовании семейства стандартов СМИБ организации могут реализовывать и совершенствовать систему управления защитой информации и подготовиться к независимой оценке их СМИБ, применяемой для защиты информации, такой как финансовая информация, интеллектуальная собственность, информация о персонале, а также информация, доверенная клиентами или третьей стороной.

Семейство стандартов СМИБ[1)] предназначено для помощи организациям любого типа и величины в реализации и функционировании СМИБ. Семейство стандартов СМИБ состоит из следующих международных стандартов под общим названием *Information technology — Security techniques (Информационные технологии. Методы и средства обеспечения безопасности)*:

- ISO/IEC 27000:2009, *Information security management systems — Overview and vocabulary (Система менеджмента информационной безопасности. Общий обзор и терминология);*
- ISO/IEC 27001:2005, *Information security management systems — Requirements (Система менеджмента информационной безопасности. Требования);*
- ISO/IEC 27002:2005, *Code of practice for information security management (Свод правил по управлению защитой информации);*
- ISO/IEC 27003, *Information security management system implementation guidance (Руководство по реализации системы менеджмента информационной безопасности);*
- ISO/IEC 27004, *Information security management — Measurement (Менеджмент информационной безопасности. Измерения);*
- ISO/IEC 27005:2008, *Information security risk management (Управление рисками информационной безопасности);*
- ISO/IEC 27006:2007, *Requirements for bodies providing audit and certification of information security management systems (Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности);*
- ISO/IEC 27007, *Guidelines for information security management systems auditing (Руководство для аудитора СМИБ)*;
- ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002).*

Примечание — Общее название «*Информационные технологии. Методы и средства обеспечения безопасности*» означает, что эти стандарты были подготовлены подкомитетом «*Методы защиты ИТ*» Совместного технического комитета ISO/IEC JTC 1 «*Информационные технологии*».

Международные стандарты, не имеющие этого общего названия:

- ISO 27799:2008, Health informatics — Information security management in health using ISO/IEC 27002 (Информатика в здравоохранении. Менеджмент информационной безопасности по стандарту ISO/IEC 27002);
- ISO/IEC 27000:2009 представляет обзор систем менеджмента информационной безопасности, которые составляют семейство стандартов СМИБ, а также дает определения терминов.

Примечание — Приложение А разъясняет, как должны интерпретироваться словесные выражения положений стандартов семейства СМИБ, выражающих требования и рекомендации.

Семейство стандартов СМИБ содержит стандарты, которые:

- определяют требования к СМИБ и к сертификации таких систем;
- содержат прямую поддержку, детальное руководство и (или) интерпретацию полных процессов «План (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA) и требования;

[1)] Перечисленные во введении стандарты, не имеющие в обозначении года выпуска, находятся в разработке.

- включают в себя специальные руководящие принципы для СМИБ;
- руководят проведением оценки соответствия СМИБ.

Глоссарий терминов и определений, приведенный в настоящем стандарте:

- охватывает термины и определения, в большинстве случаев используемые в семействе стандартов СМИБ;
- не охватывает все термины и определения, применяемые в семействе стандартов СМИБ;
- не ограничивает семейство стандартов СМИБ в определении терминов для их использования.

Стандарты, регулирующие только реализацию средств управления, в отличие от стандартов, регулирующих все меры и средства контроля и управления, содержащиеся в стандарте ISO/IEC 27002, исключены из семейства стандартов СМИБ.

Настоящий стандарт обновляется с более высокой частотой, чем обычно обновляются стандарты ИСО/МЭК, для того чтобы отразить состояние изменений семейства стандартов СМИБ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология.
Методы и средства обеспечения безопасности

СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Общий обзор и терминология

Information technology. Security techniques. Information security management systems. Overview and vocabulary

Дата введения — 2013—12—01

1 Область применения

Настоящий стандарт содержит:
- обзор семейства стандартов СМИБ;
- введение в систему менеджмента информационной безопасности (СМИБ);
- краткое описание процесса «План (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA);
- термины и определения для использования в семействе стандартов СМИБ.

Настоящий стандарт применим ко всем типам организаций (например, коммерческие предприятия, правительственные учреждения, некоммерческие организации).

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

Примечание — Термин, определяемый в каком-либо другом месте настоящего раздела, выделен жирным шрифтом. За ним в скобках следует его порядковый номер.

Пример:

Атака (attack) (2.4) определена как «попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к **активу** (2.3) или его несанкционированного использования».

Актив определен как «что-либо, что имеет ценность для организации».

Если термин **актив** заменить его определением, определение термина **атака** будет выглядеть как «попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа или несанкционированного использования чего-либо, что имеет ценность для организации».

2.1 **контроль доступа** (access control): Обеспечение того, чтобы доступ к **активам** (2.3) был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и безопасности.

2.2 **подотчетность** (accountability): Ответственность субъекта за его действия и решения.

2.3 **актив** (asset): Что-либо, что имеет ценность для организации.

Примечание — Имеются различные типы активов:
- **информация** (2.18);
- программное обеспечение;
- материальные активы, например компьютер;
- услуги;
- люди и их квалификация, навыки и опыт;
- нематериальные активы, такие как репутация и имидж.

Издание официальное

2.4 **атака** (attack): Попытка уничтожения, раскрытия, изменения, блокирования, кражи, получения несанкционированного доступа к **активу** (2.3) или его несанкционированного использования.

2.5 **аутентификация** (authentication): Обеспечение гарантии того, что заявленные характеристики объекта правильны.

2.6 **подлинность** (authenticity): Свойство, гарантирующее, что субъект или ресурс идентичен заявленному.

2.7 **доступность** (availability): Свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

2.8 **обеспечение непрерывности бизнеса** (business continuity): **Процессы** (2.31) и (или) **процедуры** (2.30), обеспечивающие уверенность в непрерывности операций бизнеса.

2.9 **конфиденциальность** (confidentiality): Свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или **процессов** (2.31).

2.10 **мера и средство контроля и управления** (control): Средство для осуществления менеджмента **риска** (2.34), включающее **политики** (2.28), **процедуры** (2.30), **рекомендации** (2.16), практические приемы или организационные структуры, которые могут иметь административный, технический, управленческий или правовой характер.

Примечание — Термин «мера и средство контроля и управления» также используется как синоним терминов «защитная мера» или «контрмера».

2.11 **цель применения мер и средств контроля и управления** (control objective): Формулировка, характеризующая, чего следует достичь в результате реализации **мер и средств контроля и управления** (2.10).

2.12 **корректирующее действие** (corrective action): Действие по устранению причины несоответствия или другой нежелательной ситуации.

[ISO 9000:2005]

2.13 **эффективность** (effectiveness): Связь между достигнутым результатом и тем, насколько целесообразно использованы ресурсы.

[ISO 9000:2005]

2.14 **результативность** (efficiency): Степень реализации запланированной деятельности и достижения запланированных результатов.

2.15 **событие** (event): Возникновение специфического набора обстоятельств.

[ISO/IEC Guide 73:2002]

2.16 **рекомендация** (guideline): Рекомендация, поясняющая действия и способы их выполнения, необходимые для достижения установленных целей.

2.17 **воздействие** (impact): Неблагоприятное изменение уровня достигнутых бизнес-целей.

2.18 **информационный актив** (information asset): Знания или данные, которые имеют значение для организации.

2.19 **информационная безопасность** (information security): сохранение **конфиденциальности** (2.9), **целостности** (2.25) и **доступности** (2.7) информации.

Примечание — Также сюда могут быть включены другие свойства, такие как **подлинность** (2.6), **подотчетность** (2.2), **неотказуемость** (2.27) и **достоверность** (2.33).

2.20 **событие в системе информационной безопасности** (information security event): Выявленное состояние системы, услуги или состояние сети, указывающее на возможное нарушение **политики** (2.28) обеспечения **информационной безопасности** (2.19), нарушение или отказ **мер и средств контроля и управления** (2.10) или прежде неизвестная ситуация, которая может иметь значение для безопасности.

2.21 **инцидент информационной безопасности** (information security incident): Одно или несколько нежелательных или неожиданных **событий информационной безопасности** (2.20), которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для **информационной безопасности** (2.19).

2.22 **менеджмент инцидента информационной безопасности** (information security incident management): **Процессы** (2.31) обнаружения, информирования, оценки, реагирования, рассмотрения и изучения **инцидентов информационной безопасности** (2.21).

2.23 **система менеджмента информационной безопасности (СМИБ)** (information security management system (ISMS): Часть общей **системы менеджмента** (2.26), основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению **информационной безопасности** (2.19).

2.24 **риск информационной безопасности** (information security risk): Потенциальная возможность того, что **уязвимость** (2.46) будет использоваться для создания **угрозы** (2.45) **активу** (2.3) или группе активов, приводящей к ущербу для организации.

2.25 **целостность** (integrity): Свойство сохранения правильности и полноты **активов** (2.3).

2.26 **система менеджмента** (management system): Система, включающая в себя **политики** (2.28), **процедуры** (2.30), **рекомендации** (2.16) и связанные с ними ресурсы для достижения целей организации.

2.27 **неотказуемость** (non-repudiation): Способность удостоверять имевшее место **событие** (2.15) или действие и их субъекты так, чтобы это **событие** (2.15) или действие и субъекты, имеющие к нему отношение, не могли быть поставлены под сомнение.

2.28 **политика** (policy): Общее намерение и направление, официально выраженное руководством.

2.29 **предупреждающее действие** (preventive action): Действие, предпринятое для устранения потенциального несоответствия или другой потенциально нежелательной ситуации.

[ISO 9000:2005]

2.30 **процедура** (procedure): Установленный способ действия или **процесса** (2.31).

[ISO 9000:2005]

2.31 **процесс** (process): Совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы.

[ISO 9000:2005]

2.32 **запись** (record): Документ, содержащий достигнутые результаты или свидетельства осуществленной деятельности.

[ISO 9000:2005]

2.33 **достоверность** (reliability): Свойство соответствия предусмотренному поведению и результатам.

2.34 **риск** (risk): Сочетание вероятности **события** (2.15) и его последствий.

[ISO/IEC Guide 73:2002]

2.35 **принятие риска** (risk acceptance): Решение принять **риск** (2.34).

[ISO/IEC Guide 73:2002]

2.36 **анализ риска** (risk analysis): Систематическое использование информации для выявления источников и оценки **риска** (2.34).

[ISO/IEC Guide 73:2002]

Примечание — Анализ риска обеспечивает базу для **оценивания риска** (2.41), **обработки риска** (2.43) и **принятия риска** (2.35).

2.37 **оценка риска** (risk assessment): общий **процесс** (2.31) **анализа риска** (2.36) и **оценивания риска** (2.41).

[ISO/IEC Guide 73:2002]

2.38 **коммуникация риска** (risk communication): Обмен информацией о **риске** (2.34) или совместное использование этой информации между лицом, принимающим решение, и другими причастными сторонами.

[ISO/IEC Guide 73:2002]

2.39 **критерии риска** (risk criteria): Правила, по которым оценивают значимость риска (2.34).

[ISO/IEC Guide 73:2002]

2.40 **количественная оценка риска** (risk estimation): Процесс присвоения значений вероятности и последствий **риска** (2.34).

[ISO/IEC Guide 73:2002]

2.41 **оценивание риска** (risk evaluation): **Процесс** (2.31) сравнения оценочной величины **риска** (2.34) с установленным **критерием риска** (2.39) с целью определения уровня значимости **риска** (2.34).

[ISO/IEC Guide 73:2002]

2.42 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении **риска** (2.34).

[ISO/IEC Guide 73:2002]

Примечание — Менеджмент риска обычно включает в себя **оценку риска** (2.37), **обработку риска** (2.43), **принятие риска** (2.35), **коммуникацию риска** (2.38), мониторинг риска и пересмотр риска.

2.43 **обработка риска** (risk treatment): **Процесс** (2.31) выбора и осуществления мер по модификации **риска** (2.34).

[ISO/IEC Guide 73:2002]

2.44 **ведомость применимости** (statement of applicability): Документ, определяющий **цели применения мер и средств контроля и управления** (2.11) и **меры и средства контроля и управления** (2.10), являющиеся адекватными и применимыми для **СМИБ** (2.23) организации.

2.45 **угроза** (threat): Возможная причина нежелательного инцидента, который может нанести ущерб системе или организации.

2.46 **уязвимость** (vulnerability): Слабое место **актива** (2.3) или **меры и средства контроля и управления** (2.10), которое может быть использовано **угрозой** (2.45).

3 Системы менеджмента информационной безопасности

3.1 Основные понятия

Организации любого типа и величины:

- собирают, обрабатывают, хранят и передают большое количество информации;
- понимают, что информация и относящиеся к ней процессы, системы, сети и персонал являются важными ресурсами для решения задач, стоящих перед организацией;
- сталкиваются с рядом рисков, которые могут оказывать воздействие на функционирование активов организации;
- ослабляют риски, осуществляя управление информационной безопасностью.

Вся информация, хранящаяся и обрабатывающаяся в организации, является объектом угроз атаки, ошибки, воздействия стихии (например, наводнения или пожара) и т. д. Термин «информационная безопасность» относится к информации, которую рассматривают как актив, у которого есть ценность, требующая соответствующей защиты, например, от потери доступности, конфиденциальности и целостности. Обеспечение возможности санкционированного своевременного получения точной и полной информации значительно повышает эффективность работы.

Защита информационных активов посредством определения, достижения, поддержания и улучшения информационной безопасности очень важна для того, чтобы позволить организации достигать свои цели, а также поддерживать и повышать уровень соответствия законодательству и репутацию. Эти скоординированные действия, направляющие реализацию подходящих средств управления и рассматривающие недопустимые риски информационной безопасности, являются общеизвестными как элементы менеджмента информационной безопасности.

Так как риски информационной безопасности и эффективность средств управления меняются в зависимости от изменяющихся обстоятельств, организациям необходимо:

- контролировать и оценивать эффективность имеющихся средств управления и процедур;
- идентифицировать появляющиеся риски для их рассмотрения;
- выбирать, реализовывать и улучшать должным образом соответствующие меры и средства контроля и управления.

Чтобы установить взаимосвязь и скоординировать такие действия системы информационной безопасности, каждая организация должна установить свою политику и цели для системы информационной безопасности и эффективно достигать эти цели при использовании системы менеджмента.

3.2 Общие положения

3.2.1 Обзор и принципы

Система менеджмента информационной безопасности (СМИБ) представляет модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов для достижения деловых целей, основанную на оценке риска и на принятии уровней риска организации, разработанную для эффективного рассмотрения и управления рисками. Анализ требований для защиты информационных активов и применение соответствующих средств управления, чтобы обеспечить необходимую защиту этих информационных активов, способствует успешной реализации СМИБ. Следующие основные принципы способствуют успешной реализации СМИБ:

- понимание необходимости системы информационной безопасности;
- назначение ответственности за информационную безопасность;
- соединение административных обязанностей и интересов заинтересованных лиц;
- возрастание социальных ценностей;

- оценка риска, определяющая соответствующие меры и средства контроля и управления для достижения допустимых уровней риска;
- безопасность как неотъемлемый существенный элемент информационных сетей и систем;
- активное предупреждение и выявление инцидентов информационной безопасности;
- обеспечение комплексного подхода к менеджменту информационной безопасности;
- непрерывная переоценка и соответствующая модификация системы информационной безопасности.

3.2.2 Информация

Информация — это актив, который наряду с другими важными деловыми активами важен для бизнеса организации и, следовательно, должен быть соответственно защищен. Информация может храниться в различных формах, включая такие как цифровая форма (например, файлы с данными, сохраненные на электронных или оптических носителях), материальная форма (например, на бумаге), а также в нематериальном виде в форме знаний служащих. Информация может быть передана различными способами: с помощью курьера, систем электронной или голосовой коммуникации. Независимо от того, в какой форме представлена информация и каким способом передается, она должна быть должным образом защищена.

Информация организации зависит от информационно-коммуникационных технологий. Эти технологии — существенный элемент в любой организации. Они облегчают создание, обработку, хранение, передачу, защиту и расширение информации. Расширение связанной глобальной деловой среды выдвигает требование защиты информации, поскольку эта информация теперь подвергается воздействию более широкого разнообразия угроз и уязвимостей.

3.2.3 Информационная безопасность

Информационная безопасность включает в себя три основных измерения: конфиденциальность, доступность и целостность. С целью обеспечения длительного непрерывного успеха в бизнесе и уменьшения нежелательных воздействий информационная безопасность предусматривает применение соответствующих мер безопасности, которые включают в себя рассмотрение широкого диапазона угроз, а также управление этими мерами.

Информационная безопасность достигается посредством применения соответствующего набора средств управления, определенного с помощью процесса управления рисками и управляемого с использованием СМИБ, включая политику, процессы, процедуры, организационные структуры, программное и аппаратное обеспечение, чтобы защитить идентифицированные информационные активы. Эти меры и средства контроля и управления должны быть определены, реализованы, проверены, проанализированы и при необходимости улучшены, чтобы гарантировать, что уровень безопасности соответствует деловым целям организации. Меры и средства контроля и управления безопасностью важной информации неразрывно связываются с бизнес-процессами организации.

3.2.4 Менеджмент

Менеджмент включает в себя действия по управления, контролю и непрерывному совершенствованию организации в рамках соответствующих структур. Управленческие действия включают в себя действия, методы или практику формирования, обработки, направления, наблюдения и управления ресурсами. Величина управленческой структуры может варьироваться от одного человека в небольших организациях до управленческой иерархии в крупных организациях, состоящих из многих людей.

Относительно СМИБ менеджмент включает в себя наблюдение и выработку решений, необходимых для достижения деловых целей посредством защиты информационных активов организации. Менеджмент информационной безопасности выражается через формулирование и использование политики информационной безопасности, стандартов, процедур и рекомендаций, которые применяются повсеместно в организации всеми лицами, связанными с ней.

Примечание —Термин «менеджмент» может иногда относиться к людям (то есть к человеку или группе людей с властью и ответственностью за управление и контроль организации). Термин «менеджмент», употребляемый в этом пункте, имеет другой смысл.

3.2.5 Система менеджмента

Система менеджмента использует совокупность ресурсов для достижения целей организации. Система менеджмента включает в себя организационную структуру, политику, планирование действий, обязательства, методы, процедуры, процессы и ресурсы.

В части информационной безопасности система управления позволяет организации:
- удовлетворять требования безопасности клиентов и других заинтересованных лиц;
- улучшать планы и действия организации;
- соответствовать целям информационной безопасности организации;

- выполнять регулирующие требования, требования законодательства и отраслевые нормативные документы;
- организованно управлять информационными активами для облегчения непрерывного совершенствования и регулирования текущих организационных целей и внешних условий.

3.3 Процессный подход для СМИБ

Организации нужно вести различные виды деятельности и управлять ими для того, чтобы функционировать результативно. Любой вид деятельности, использующий ресурсы и управляемый для того, чтобы обеспечить возможность преобразования входов в выходы, можно считать процессом. Выход одного процесса может непосредственно формировать вход следующего процесса. Обычно такая трансформация происходит в условиях планирования и управления. Применение системы процессов в рамках организации вместе с идентификацией и взаимодействием этих процессов, а также их управлением может быть определено как «процессный подход».

Процессный подход для СМИБ, представленный в семействе стандартов СМИБ, основан на операционном принципе, принятом в стандартах системы управления ISO и общеизвестном как процесс «План (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA):

- план — постановка целей и разработка планов (провести анализ ситуации в организации, наметить общие цели, поставить задачи и разработать планы для их достижения);
- осуществление — реализация планов (выполнить то, что было запланировано);
- проверка — проверка результатов (измерение/контроль степени соответствия достигнутых результатов плану);
- действие — коррекция и улучшение работы (учиться на ошибках, чтобы улучшить работу и достичь лучших результатов).

3.4 Цели внедрения СМИБ

В качестве части СМИБ организации должны быть определены риски, связанные с информационными активами организации. Достижение информационной безопасности требует управления риском и охватывает риски физические, человеческие и технологические, относящиеся к угрозам, касающимся всех форм информации внутри организации или используемой организацией.

Принятие СМИБ является стратегическим решением для организации, и необходимо, чтобы это решение неразрывно интегрировалось, оценивалось и обновлялось в соответствии с потребностями организации.

На разработку и реализацию СМИБ организации влияют потребности и цели организации, требования безопасности, используемые бизнес-процессы, а также размер и структура организации. Разработка и функционирование СМИБ должны отражать интересы и требования информационной безопасности всех заинтересованных лиц организации, включая клиентов, поставщиков, деловых партнеров, акционеров и других третьих лиц.

Во взаимосвязанном мире информация и относящиеся к ней процессы, системы и сети составляют критические деловые активы. Организации и их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, а также пожар и наводнение. Повреждения информационных систем и сетей, вызванные вредоносным кодом, действиями хакеров и DoS-атаками, стали более распространенными, более масштабными и все более и более серьезными.

СМИБ важна для предприятий как государственного, так частного сектора. В любой отрасли СМИБ является необходимым инструментом для поддержания электронного бизнеса и важна для действий менеджмента риска. Взаимосвязь общедоступных и частных сетей и распределенность информационных активов увеличивают трудность управления доступом к информации и ее обработки. Кроме того, распространение мобильных устройств хранения данных, содержащих информационные активы, может ослабить эффективность традиционных средств контроля. Когда организации принимают семейство стандартов СМИБ, способность применить последовательные и взаимно известные принципы информационной безопасности может быть продемонстрирована деловым партнерам и другим заинтересованным сторонам.

Информационная безопасность не всегда учитывается при проектировании и расширении информационных систем. Кроме того, часто считают, что информационная безопасность — это техническая проблема. Однако уровень безопасности, который может быть достигнут с помощью технических средств, ограничен. Такая защита может быть неэффективной, не будучи поддержанной соответствующим управлением и процедурами в контексте СМИБ. Последующее встраивание системы безопасности в информационную систему может быть трудным и дорогостоящим. СМИБ включает в себя идентификацию имеющихся средств управления и требует тщательного планирования и внимания к деталям.

Например, средства контроля доступа, которые могут быть техническими (логическими), физическими, административными (организационными), или их комбинация гарантируют, что доступ к информационным активам разрешен и ограничен на основании требований бизнеса и требований безопасности.

Принятие СМИБ важно для защиты информационных активов. Это позволяет организации:

- повысить гарантии того, что ее информационные активы в достаточной мере на непрерывной основе защищены от угроз информационной безопасности;
- поддерживать структурированную и всестороннюю систему для идентификации и оценки угроз информационной безопасности, выбора и применения соответствующих средств управления и измерения и улучшения их эффективности;
- непрерывно улучшать ее среду контроля;
- соответствовать юридическим и регулирующим требованиям.

3.5 Внедрение, контроль, поддержка и улучшение СМИБ

3.5.1 Общие положения

Организация должна предпринимать следующие меры по внедрению, контролю, поддержке и улучшению ее СМИБ:

- определение информационных активов и связанных с ними требований безопасности (см. 3.5.2);
- оценка рисков информационной безопасности (см. 3.5.3);
- выбор и реализация соответствующих средств управления для управления неприемлемыми рисками (см. 3.5.4);
- контроль, поддержка и повышение эффективности средств управления безопасностью, связанных с информационными активами организации (см. 3.5.5).

Для гарантии эффективной непрерывной защиты информационных активов организации с помощью СМИБ необходимо постоянно повторять шаги (a) — (d), чтобы выявлять изменения рисков, стратегии организации или деловых целей.

3.5.2 Определение требований информационной безопасности

В пределах общей стратегии и деловых целей организации, ее размера и географического распространения требования информационной безопасности могут быть определены при анализе следующих факторов:

- идентифицированные информационные активы и их ценность;
- деловые потребности в обработке и хранении информации;
- юридические, регулирующие и договорные требования.

Проведение методической оценки рисков, связанных с информационными активами организации, включает в себя анализ угроз информационным активам, уязвимостей информационных активов и вероятности угрозы информационным активам, потенциального воздействия любого инцидента информационной безопасности на информационные активы. Расходы на соответствующие меры и средства контроля и управления безопасностью пропорциональны оцениваемому деловому воздействию в случае осуществления риска.

3.5.3 Оценка рисков информационной безопасности

Управление рисками информационной безопасности требует соответствующей оценки риска и метода обработки риска. Это может включать в себя оценку затрат и преимуществ, законных требований, социальных, экономических и экологических аспектов, проблем заинтересованных лиц, приоритетов и других входов и переменных. Результаты оценки риска информационной безопасности помогут выработать и провести соответствующие управленческие решения для действий и установления приоритетов для управления рисками информационной безопасности, а также для реализации соответствующих средств управления безопасностью для защиты от этих рисков. Стандарт ISO/IEC 27005 обеспечивает руководство менеджментом рисков информационной безопасности, включая рекомендации относительно оценки риска, обработки риска, принятия риска, коммуникации риска, контроля риска и анализа риска.

3.5.4 Выбор и реализация средств управления информационной безопасностью

После определения требований к информационной безопасности и оценки рисков информационной безопасности для идентифицированных информационных активов (включая решения для обработки рисков информационной безопасности) должны быть выбраны и реализованы соответствующие меры и средства контроля и управления, чтобы гарантировать, что риски информационной безопасности уменьшены до уровня, приемлемого для организации. Меры и средства контроля и управления могут быть выбраны с помощью стандарта ISO/IEC 27002 или из других соответствующих наборов средств управления. Также для удовлетворения специфических потребностей могут быть разработаны новые

соответствующие меры и средства контроля и управления. Выбор средств управления безопасностью зависит от требований безопасности, принимающих во внимание критерии для принятия риска информационной безопасности, вариантов обработки риска и общего подхода управления рисками, применяемого организацией. Выбор и реализация средств управления могут быть документированы в заявлении о применимости.

Меры и средства контроля и управления, изложенные в ISO/IEC 27002, общепризнаны как лучшие методы, применимые к большинству организаций. Они были разработаны для того, чтобы удовлетворять требованиям организаций разной величины и структуры. Другие стандарты семейства стандартов СМИБ руководят выбором и применением средств управления информационной безопасностью, изложенных в стандарте ISO/IEC 27002, для системы менеджмента (ISO/IEC 27001).

3.5.5 Контроль, поддержка и повышение эффективности СМИБ

Организация должна поддерживать работоспособность и улучшать СМИБ посредством контроля и оценки деятельности, направленной против политики и целей организации, и сообщения о результатах менеджменту для анализа. Этот анализ СМИБ позволит наглядно показать правильность и отслеживаемость корректирующих, профилактических действий и действий по усовершенствованию, основанных на этих результатах, включая контроль средств управления информационной безопасностью.

3.6 Критические факторы успеха СМИБ

Для успешной реализации СМИБ, позволяющей организации достичь своих деловых целей, имеет значение большое количество факторов. Примеры критических факторов успеха включают в себя следующие:

- политика информационной безопасности, цели и действия, ориентированные на достижение целей;
- методика и структура для разработки, реализации, контроля, поддержания и улучшения информационной безопасности, которые соответствуют корпоративной культуре;
- видимая поддержка и обязательства со стороны всех уровней управления, особенно высшего руководства;
- понимание требований информационной защиты активов, достигаемое через применение менеджмента рисков информационной безопасности (см. стандарт ISO/IEC 27005);
- эффективное информирование об информационной безопасности, обучение и образовательная программа, доводящая до сведения всех служащих и других причастных сторон их обязательства по информационной безопасности, сформулированные в политике информационной безопасности, стандартах и т. д., а также их мотивирование к соответствующим действиям;
- эффективный процесс менеджмента инцидентов информационной безопасности;
- эффективный управленческий подход непрерывности бизнеса;
- система измерения, которая используется для оценки управления информационной безопасностью, и предложения по улучшению, поступающие по цепочке обратной связи.

СМИБ увеличивает вероятность того, что организация будет последовательно достигать решающих факторов успеха, необходимых для защиты ее информационных активов.

3.7 Преимущества внедрения стандартов семейства СМИБ

Преимущества реализации СМИБ вытекают, прежде всего, из сокращения рисков информационной безопасности (то есть уменьшения вероятности воздействия и (или) уменьшения воздействия, вызванного инцидентами информационной безопасности). В частности, преимущества, полученные от принятия семейства стандартов СМИБ, включают в себя следующее:

- поддержка процесса определения, реализации, функционирования и поддержания работоспособности полной и экономически эффективной комплексной СМИБ, которая удовлетворяет потребности организации;
- помощь для руководства в структурировании его подхода к менеджменту информационной безопасности в контексте корпоративного менеджмента рисков и управления, включая обучение и тренинг по единому управлению информационной безопасностью;
- продвижение общепринятых лучших методов информационной безопасности в необязывающей форме, что предоставляет организациям свободу для принятия и улучшения средств управления, которые соответствуют их особенностям и оказывают им поддержку перед лицом внутренних и внешних изменений;
- предоставление общего языка и концептуального основания для информационной безопасности, что облегчает взаимопонимание с деловыми партнерами, особенно если они требуют свидетельства соответствия ISO/IEC 27001 от аккредитованного органа сертификации.

4 Семейство стандартов СМИБ

4.1 Общая информация

Семейство стандартов СМИБ состоит из взаимосвязанных стандартов, изданных или разрабатываемых, и содержит несколько существенных структурных компонентов. Эти компоненты изложены в нормативных стандартах, описывающих требования СМИБ (ISO/IEC 27001) и требования для организаций, сертифицирующих соответствие стандарту ISO/IEC 27001 (ISO/IEC 27006). Другие стандарты обеспечивают руководство при различных аспектах реализации СМИБ, включая в себя общий процесс, рекомендации, относящиеся к управлению, а также специальные руководства. Взаимосвязь внутри семейства стандартов СМИБ[2)] показана на рисунке 1.

Стандарты, которые содержат прямую поддержку, детализированное руководство и (или) толкование для общего процесса PDCA и требований, заданных в ISO/IEC 27001 (см. 4.3.1), ISO/IEC 27000 (см. 4.2.1), ISO/IEC 27002 (см. 4.4.1), ISO/IEC 27003 (см. 4.4.2), ISO/IEC 27004 (см. 4.4.3), ISO/IEC 27005 (см. 4.4.4) и ISO/IEC 27007 (см. 4.4.5).

Стандарт ISO/IEC 27006 (см. 4.3.2) содержит требования для органов, проводящих сертификацию СМИБ.

Стандарты ISO/IEC 27011 (см. 4.5.1) и ISO 27799 (см. 4.5.2) включают в себя специальные рекомендации для СМИБ[3)].

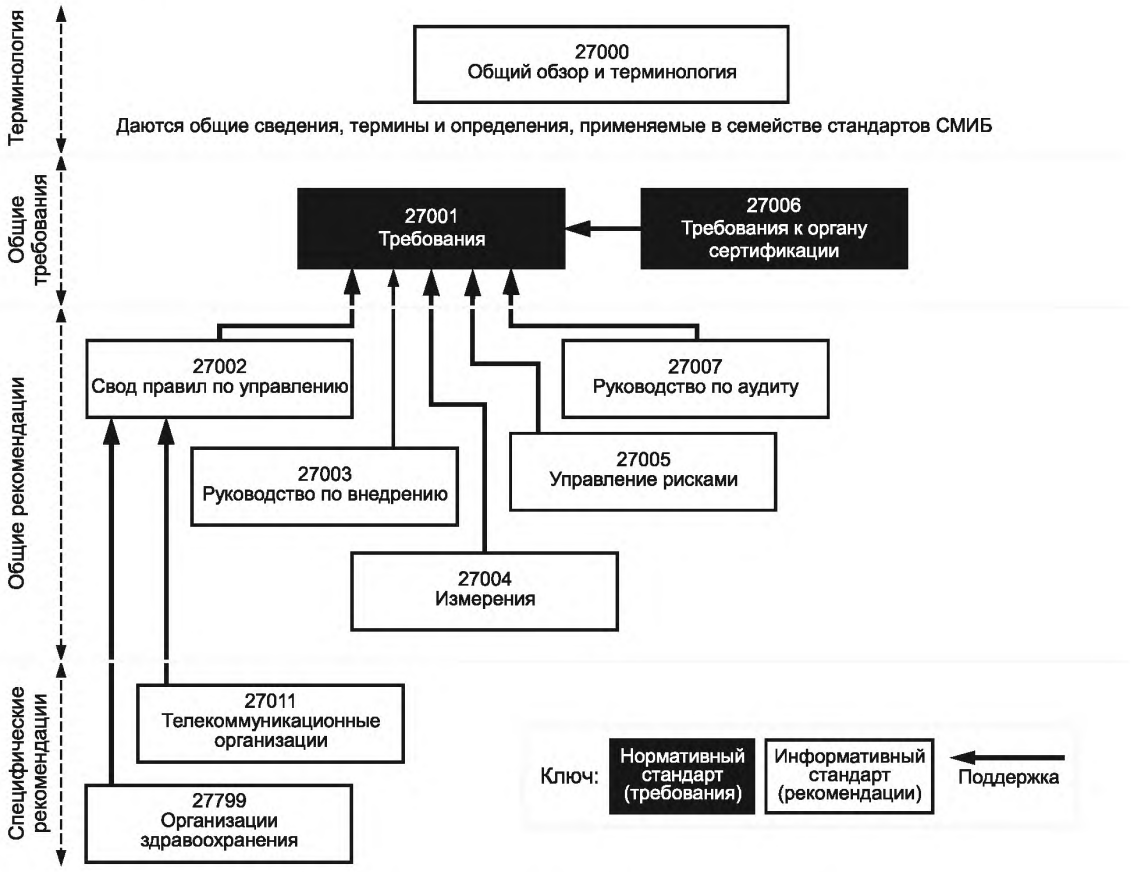

Рисунок 1 — Взаимосвязь в семействе стандартов СМИБ

[2)] ISO/IEC 27003, ISO/IEC 27004 и ISO/IEC 27007 находятся в разработке.

[3)] Обозначения ISO/IEC 27008, ISO/IEC 27009 и ISO/IEC 27010 зарезервированы для последующей разработки стандартов семейства СМИБ, по которым не было принято решение к моменту публикации настоящего стандарта.

Семейство стандартов СМИБ поддерживает взаимосвязь со многими другими стандартами ISO и ISO/IEC. Стандарты СМИБ классифицируются по следующим признакам:

- стандарты, содержащие общий обзор и терминологию (см. 4.2);
- стандарты, задающие требования (см. 4.3);
- стандарты, содержащие общие рекомендации (см. 4.4);
- стандарты, содержащие специальные рекомендации (см. 4.5).

4.2 Стандарты, содержащие общий обзор и терминологию

4.2.1 ISO/IEC 27000 настоящий стандарт

Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

Область применения. Этот международный стандарт содержит:

- обзор семейства стандартов СМИБ;
- введение в систему менеджмента информационной безопасности (СМИБ);
- краткое описание процесса «План (Plan) — Осуществление (Do) — Проверка (Check) — Действие (Act)» (PDCA);
- термины и определения для использования в семействе стандартов СМИБ.

Назначение: ISO/IEC 27000 описывает основы системы менеджмента информационной безопасности, которая составляет предмет семейства стандартов СМИБ, и определяет относящиеся к ней термины.

4.3 Стандарты, задающие требования

4.3.1 ISO/IEC 27001

Информационная технология. Средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Область применения: этот международный стандарт определяет требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной СМИБ в контексте общих деловых рисков организации. Он определяет требования для реализации средств управления защитой, приспособленных к потребностям отдельных организаций или их подразделений. Этот международный стандарт применим ко всем типам организаций (например, коммерческие, государственные, некоммерческие организации).

Назначение: ISO/IEC 27001 содержит нормативные требования для развертывания и функционирования СМИБ, включая набор средств управления для управления и уменьшения рисков, относящихся к информационным активам, которые организация стремится защитить. Организации, использующие СМИБ, могут проводить ее аудиторскую проверку и сертификацию соответствия. Цели управления и мера и средства контроля и управления из приложения А стандарта ISO/IEC 27001 должны быть выбраны как часть этого СМИБ-процесса для того, чтобы удовлетворять определенные требования.

Цели управления, меры и средства контроля и управления, перечисленные в таблице А.1 стандарта ISO/IEC 27001, получены непосредственно из перечня целей управления и средств управления, перечисленных в разделах 5—15 ISO/IEC 17799:2005, и согласованы с ними.

4.3.2 ISO/IEC 27006

Информационная технология. Средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности

Область применения: этот международный стандарт задает требования и является руководством для органов, проводящих аудит и сертификацию СМИБ на соответствие ISO/IEC 27001 в дополнение к требованиям, содержащимся в ISO/IEC 17021. Этот стандарт предназначен главным образом для проведения аккредитации органов, проводящих сертификацию СМИБ на соответствие ISO/IEC 27001.

Назначение: ISO/IEC 27006 дополняет стандарт ISO/IEC 17021 в части требований для аккредитации органов сертификации, проводящих сертификацию соответствия требованиям, изложенным в стандарте ISO/IEC 27001.

4.4 Стандарты, содержащие общие рекомендации

4.4.1 ISO/IEC 27002

Информационная технология. Средства обеспечения безопасности. Свод правил по управлению защитой информации

Область применения: этот международный стандарт содержит перечень общепринятых целей управления и лучшие методы реализации средств управления для использования в качестве руководства при выборе и внедрении средств управления для достижения информационной безопасности.

Назначение: ISO/IEC 27002 является руководством по внедрению средств управления защитой информации. В частности, разделы 5—15 содержат специальные рекомендации и руководство по реализации средств управления, приведенных в разделах А.5 — А.15 стандарта ISO/IEC 27001.

4.4.2 ISO/IEC 27003

Информационная технология. Средства обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности

Область применения: этот международный стандарт будет содержать практическое руководство по внедрению и включать в себя расширенную информацию по созданию, эксплуатации, контролю, анализу, поддержке и улучшению СМИБ в соответствии со стандартом ISO/IEC 27001.

Назначение: ISO/IEC 27003 будет содержать описание процессного подхода к внедрению СМИБ в соответствии со стандартом ISO/IEC 27001.

4.4.3 ISO/IEC 27004

Информационная технология. Средства обеспечения безопасности. Измерения

Область применения: этот международный стандарт будет включать в себя руководство и рекомендации по совершенствованию и использованию измерений для оценки эффективности СМИБ, целей управления, средств управления, применяемых при обеспечении информационной безопасности и управлении информационной безопасностью в соответствии со стандартом ISO/IEC 27001.

Назначение: ISO/IEC 27004 будет содержать систему измерений, позволяющую определять оценку эффективности СМИБ в соответствии со стандартом ISO/IEC 27001.

4.4.4 ISO/IEC 27005

Информационная технология. Средства обеспечения безопасности. Управление рисками информационной безопасности

Область применения: этот стандарт включает в себя рекомендации для менеджмента рисков информационной безопасности. Методы, описанные в этом стандарте, соответствуют общим принципам, изложенным в ISO/IEC 27001.

Назначение: ISO/IEC 27005 содержит руководство по внедрению процессного подхода к управлению рисками для полного выполнения требований стандарта ISO/IEC 27001, относящихся к управлению рисками информационной безопасности.

4.4.5 ISO/IEC 27007

Информационная технология. Средства обеспечения безопасности. Руководство для аудитора СМИБ

Область применения: этот международный стандарт будет включать в себя руководство по проведению аудита СМИБ, а также руководство по оценке компетентности аудиторов системы менеджмента информационной безопасности в дополнение к руководству, содержащемуся в стандарте ISO 19011, который относится к системам менеджмента в целом.

Назначение: ISO/IEC 27007 будет содержать руководство для организаций, которым необходимо проводить внутренний или внешний аудит СМИБ или управлять программой проведения аудита СМИБ в соответствии с требованиями стандарта ISO/IEC 27001.

4.5 Стандарты, описывающие рекомендации для специальной области

4.5.1 ISO/IEC 27011

Информационная технология. Средства обеспечения безопасности. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002

Область применения: этот международный стандарт содержит руководящие указания по реализации управления защитой информации в телекоммуникационных организациях.

Назначение: ISO/IEC 27011 предоставляет телекоммуникационным организациям руководящие указания на основе стандарта ISO/IEC 27002 с учетом специфики данной отрасли и дополняет его руководящие указания по выполнению требований, изложенных в приложении А стандарта ISO/IEC 27001.

4.5.2 ISO 27799

Информатика в здравоохранении. Менеджмент информационной безопасности по стандарту ISO/IEC 27002

Область применения: этот международный стандарт содержит руководящие указания по реализации управления защитой информации в организациях здравоохранения.

Назначение: ISO/IEC 27799 предоставляет организациям здравоохранения руководящие указания на основе стандарта ISO/IEC 27002 с учетом специфики данной отрасли и дополняет его руководящие указания по выполнению требований, изложенных в приложении А стандарта ISO/IEC 27001.

Приложение А
(справочное)

Глагольные формы, используемые для формулировок положений стандартов

Каждый из документов семейства стандартов СМИБ не требует обязательного его исполнения. Однако такие обязательства могут налагаться, например, законодательством или контрактом. Чтобы иметь соответствие с нормативными документами, пользователю нужно выделять требования, которые обязательно должны быть удовлетворены, и отличать эти требования от рекомендаций, которые дают определенную свободу выбора.

Таблица А.1 разъясняет, как должны интерпретироваться словесные выражения положений стандартов семейства СМИБ, выражающих требования и рекомендации.

Таблица А.1 — Интерпретация словесных выражений положений стандартов семейства СМИБ, выражающих требования и рекомендации

УКАЗАНИЕ	ПОЯСНЕНИЕ
Требование	Слова «shall» и «shall not» выражают требования, которым необходимо строго соответствовать и от которых не допускается никаких отклонений
Рекомендация	Слова «should» и «should not» означают, что рекомендуется как наиболее подходящий один вариант из нескольких возможных, не исключая другие варианты, или что определенный план предпочтителен, но необязателен, или (в отрицательной форме) что определенная возможность или план действий нежелателен, но не запрещен
Разрешение	Слова «may» и «need not» означают, что план действий допустим в пределах данного документа
Возможность	Слова «can» и «cannot» указывают на возможность чего-либо

Приложение В
(справочное)

Перечень терминов по категориям

В.1 Термины, относящиеся к информационной безопасности

2.2 Подотчетность (accountability).
2.5 Аутентификация (authentication).
2.6 Подлинность (authenticity).
2.7 Доступность (availability).
2.9 Конфиденциальность (confidentiality).
2.19 Информационная безопасность (information security).
2.25 Целостность (integrity).
2.27 Неотказуемость (non-repudiation).
2.33 Достоверность (reliability).

В.2 Термины, относящиеся к менеджменту

2.8 Непрерывность бизнес-процессов (business continuity).
2.12 Корректирующее действие (corrective action).
2.13 Эффективность (effectiveness).
2.14 Результативность (efficiency).
2.16 Рекомендация (guideline).
2.23 Система менеджмента информационной безопасности (СМИБ) (information security management system (ISMS).
2.26 Система менеджмента (management system).
2.28 Политика (policy).
2.29 Предупреждающее действие (preventive action).
2.31 Процесс (process).

В.3 Термины, относящиеся к риску информационной безопасности

2.1 Контроль доступа (access control).
2.3 Актив (asset).
2.4 Атака (attack).
2.10 Мера и средство контроля и управления (control).
2.11 Цель применения мер и средств контроля и управления (control objective).
2.15 Событие (event).
2.17 Воздействие (impact).
2.18 Информационный актив (information asset).
2.20 Событие в системе информационной безопасности (information security event).
2.21 Инцидент информационной безопасности (information security incident).
2.22 Менеджмент инцидента информационной безопасности (information security incident management).
2.24 Риск информационной безопасности (information security risk).
2.34 Риск (risk).
2.35 Принятие риска (risk acceptance).
2.36 Анализ риска (risk analysis).
2.37 Оценка риска (risk assessment).
2.38 Коммуникация риска (risk communication).
2.39 Критерий риска (risk criteria).
2.40 Количественная оценка риска (risk estimation).
2.41 Оценивание риска (risk evaluation).
2.42 Менеджмент риска (risk management).
2.43 Обработка риска (risk treatment).
2.45 Угроза (threat).
2.46 Уязвимость (vulnerability).

В.4 Термины, относящиеся к документации

2.30 Процедура (procedure).
2.32 Запись (record).
2.44 Ведомость применимости (statement of applicability).

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ISO/IEC 27006:2007	IDT	ГОСТ Р ИСО/МЭК 27006—2008 «Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности»
ISO/IEC 27005:2008	IDT	ГОСТ Р ИСО/МЭК 27005—2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
Примечание —В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 17021:2006, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[4] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[5] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

[6] ISO/IEC 27003[4], *Information technology — Security techniques — Information security management system implementation guidance*

[7] ISO/IEC 27004[5], *Information technology — Security techniques — Information security management — Measurement*

[8] ISO/IEC 27005:2008, *Information technology — Security techniques — Information security risk management*

[9] ISO/IEC 27006:2007*, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[10] ISO/IEC 27007[6], *Information technology — Security techniques — Guidelines for information security management systems auditing*

[11] ISO/IEC 27011[7], *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*

[12] ISO 27799:2008, *Health informatics — Information security — management in health using ISO/IEC 27002*

[13] ISO/IEC Guide 73:2002*, Risk Management — Vocabulary — Guidelines for use in standards*

[4] Будет опубликован.

[5] Будет опубликован.

[6] Будет опубликован.

[7] Будет опубликован.

УДК 004.91:006.354 ОКС 35.040
01.040.35

Ключевые слова: система менеджмента информационной безопасности, документально оформленная процедура, инцидент информационной безопасности

Редактор *А.В. Барандеев*
Технический редактор *В.Н. Прусакова*
Корректор *М.С. Кабашова*
Компьютерная верстка *Ю.В. Демениной*

Сдано в набор 14.04.2014. Подписано в печать 06.05.2014. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,25. Тираж 96 экз. Зак. 1591.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru