МЕЖДУНАРОДНЫЙ СТАНДАРТ

ISO/IEC 27000

Пятая редакция
2018-02

Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Номер для ссылки
ISO/IEC 27000:2018 (E)

Логотип ISO | Логотип IEC

ДОКУМЕНТ С ЗАЩИЩЕННЫМ АВТОРСКИМ ПРАВОМ

Бюро ISO по охране авторских прав
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
www.iso.org

Издано в Швейцарии

Оглавление

Страница

Предисловие

ISO (International Organization for Standardization – Международная Организация по Стандартизации) является всемирной федерацией национальных органов по стандартизации (органов-членов ISO). Работа над подготовкой Международных Стандартов выполняется, как правило, техническими комитетами ISO. Каждый орган-член ISO, заинтересованный в цели, для которой был создан технический комитет, имеет право быть представленным в данном комитете. Международные организации, правительственные и неправительственные, поддерживающие связь с ISO, также принимают участие в работе. ISO также тесно сотрудничает с Международной Электротехнической Комиссией (IEC), ведется совместная работа по всем вопросам электротехнической стандартизации.

Процедуры, использованные при разработке этого документа и предназначенные для дальнейшей поддержки, описаны в Директивах ISO/IEC, Часть 1. В частности, должны быть указаны различные критерии утверждения, необходимые для различных типов документов ISO. Настоящий документ был разработан в соответствии с правилами, изложенными в Директивах ISO/IEC, Часть 2 (см. www.iso.org/directives).

Особое внимание уделено тому, что некоторые элементы данного документа могут являться предметом патентных прав. ISO не должна нести ответственность за идентификацию какого-либо или всех подобных патентных прав. Детали, касающиеся любых патентных прав, установленные в ходе разработки документа, должны быть указаны в разделе Введение и/или в листе патентных деклараций ISO (см. www.iso.org/patents).

Все торговые марки, упомянутые в настоящем документе, приведены для удобства пользователей и не означают рекомендации (одобрения).

Для разъяснения значений, используемых ISO специфических терминов и выражений, связанных с оценкой соответствия, равно как и информации о соблюдении ISO принципов соглашения Всемирной Торговой Организации (ВТО) по техническим барьерам в торговле (ТБТ) см. следующую ссылку: Foreword – Supplementary information.

Данный документ был разработан Техническим комитетом ISO/IEC JTC 1, Информационные технологии, Подкомитет SC 27, Методы обеспечения безопасности в ИТ.

Данная пятая редакция отменяет и заменяет четвертую редакцию (ISO/IEC 27000:2016), которая была технически пересмотрена. Основные изменения по сравнению с предыдущей редакцией следующие:

- было переработано Введение,
- были удалены некоторые термины и определения,
- раздел 3 был приведен в соответствие со структурой высокого уровня стандартов на системы менеджмента,
- раздел 5 был обновлен, чтобы отразить изменения в соответствующих стандартах,
- были удалены приложения A и B.

Введение

0.1 Обзор

Международные стандарты на системы менеджмента предлагают модель для применения при построении и функционировании системы менеджмента. Эта модель включает в себя элементы, которые экспертами в данной области на основе консенсуса признаны лучшей международной практикой. Подкомитет ISO/IEC JTC 1/SC 27 играет роль экспертного комитета, осуществляющего развитие международных стандартов на системы менеджмента в области информационной безопасности, иначе известных как семейство стандартов на Системы Менеджмента Информационной Безопасности (СМИБ).

Используя это семейство стандартов, организации могут разрабатывать и поддерживать среду для управления безопасностью их информационных активов, включая финансовую информацию, интеллектуальную собственность, данные о работниках, или информацию, доверенную им клиентами или третьими лицами. Эти стандарты также могут использоваться для подготовки к независимой оценке их СМИБ, применяемой для защиты информации.

0.2 Назначение данного документа

Семейство стандартов на СМИБ включает стандарты, которые:

a) определяют требования к СМИБ и тем, кто сертифицирует такие системы;

b) обеспечивают непосредственную поддержку, содержат подробные рекомендации и/или интерпретацию общего процесса разработки, внедрения, обеспечения работоспособности и улучшения СМИБ;

c) содержат руководства по СМИБ для конкретных отраслей; и

d) содержат указания по оценке соответствия СМИБ.

0.3 Значение некоторых глаголов в данном документе

В данном документе используются следующие формы глаголов:

- «shell» (должна, должно) указывает на требование;
- «should» (следует) указывает на рекомендацию;
- «may» (может, разрешено) указывает на допустимость;
- «can» (может, имеет возможность) указывает на возможность или способность.

Информация, отмеченная как «ПРИМЕЧАНИЕ», дается для улучшения понимания и пояснения соответствующего требования. Примечания к определениям Раздела 3 содержат информацию, которая дополняет терминологические данные и может содержать положения, касающиеся использования термина.

Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь

1 Область применения

Данный документ содержит общие сведения по системам менеджмента информационной безопасности (СМИБ). Он также содержит термины и определения, широко используемые в семействе стандартов на СМИБ. Данный документ применим для всех типов и размеров организацией (например, коммерческих предприятий, правительственных учреждений, некоммерческих организаций).

Термины и определения, используемые в данном документе:

- включают в себя обычно используемые в семействе стандартов на СМИБ термины и определения;
- не охватывают всех терминов и определений, применяемых в семействе стандартов на СМИБ; и
- не ограничивают семейство стандартов на СМИБ в определении новых терминов.

2 Нормативные ссылки

Данный документ не содержит нормативных ссылок.

3 Термины и определения

ISO и IEC поддерживают терминологическую базу данных для применения в сфере стандартизации по следующим адресам:

- платформа ISO Online browsing: доступна на http://www.iso.org/obp
- IEC Electropedia: доступна на http://www.electropedia.org/

3.1

управление доступом (access control)

средства, призванные гарантировать, что доступ к активам разрешен и ограничен в соответствии с *требованиями* (3.56) бизнеса и безопасности

3.2

атака (attack)

попытка уничтожить, раскрыть, изменить, сделать недоступным, украсть или получить несанкционированный доступ к активу или несанкционированно использовать его

3.3

аудит (audit)

систематический, независимый и документированный *процесс* (3.54) получения свидетельства аудита и объективной его оценки с целью определения степени, с которой выполняются критерии аудита

Примечание 1 к определению: Аудит может быть внутренним (первой стороны) или внешним (второй или третьей стороны), а также может быть комбинированным аудитом (объединяющим два или более направления)

Примечание 2 к определению: Внутренний аудит проводится самой организацией или внешней стороной в интересах организации

Примечание 3 к определению: Термины «свидетельство аудита» и «критерий аудита» определены в ISO 19011.

3.4

область аудита (audit scope)

объем и границы *аудита* (3.3)

[ИСТОЧНИК: ISO 19011:2011, 3.14, изменено – удалено Примечание 1 к определению]

3.5

аутентификация (authentication)

обеспечение гарантии того, что заявленная характеристика объекта является подлинной

3.6

подлинность (authenticity)

свойство, указывающее, что объект представляет собой то, что он заявляет о себе

3.7

возможность применения (availability)

свойство доступности и готовности к использованию по запросу авторизованного объекта

3.8

основной показатель (base measure)

показатель (3.42), определенный через атрибут и метод его количественной оценки

Примечание 1 к определению: Основной показатель функционально не зависит от других *показателей*

[ИСТОЧНИК: ISO/IEC/IEEE 15939:2017, 3.3, изменено – удалено Примечание 2 к определению]

3.9

компетентность (competence)

способность применять знания и навыки для достижения желаемых результатов

3.10

конфиденциальность (confidentiality)

состояние, при котором обеспечивается недоступность или нераскрытие информации неавторизованным частным или юридическим лицам или *процессам* (3.54)

3.11

соответствие (conformity)

выполнение *требования* (3.56)

3.12

последствие (consequence)

результат *события* (3.21), оказывающий влияние на *цели* (3.49)

Примечание 1 к определению: Событие может вызывать ряд последствий

Примечание 2 к определению: Последствие может быть известным или неизвестным и в контексте информационной безопасности, как правило, является негативным

Примечание 3 к определению: Последствия могут оцениваться количественно или качественно

Примечание 4 к определению: Первоначальные последствия могут усугубляться эффектом цепной реакции

[ИСТОЧНИК: ISO Guide 73:2009, 3.6.1.3, измененный – В Примечание 2 к определению внесено изменение после союза «и»]

3.13

постоянное улучшение (continual improvement)

повторяющаяся деятельность по улучшению *показателей деятельности* (3.52)

3.14

средство управления (control)

воздействие, которое изменяет *риск* (3.61)

Примечание 1 к определению: К средствам управления относится любой *процесс* (3.54), *политика* (3.53), применение устройства, установившаяся практика или другие действия, которые изменяют *риск* (3.61).

Примечание 2 к определению: Средства управления не всегда могут приводить к запланированным или предполагаемым изменениям

[ИСТОЧНИК: ISO Guide 73:2009, 3.8.1.1 – Примечание 2 к определению изменено]

3.15

цель управления (control objective)

описание того, что должно быть достигнуто в результате применения *средств управления* (3.14)

3.16

коррекция (correction)

действие для устранения обнаруженного *несоответствия* (3.47)

3.17

корректирующее действие (corrective action)

действие для устранения причины *несоответствия* (3.47) и предотвращения ее повторного проявления

3.18

производный показатель (derived measure)

показатель (3.42), который определяется как функция двух или более значений *основных показателей* (3.8)

[ИСТОЧНИК: ISO/IEC 15939:2007, 2.8 – удалено Примечание 1 к определению]

3.19

документированная информация (documented information)

информация, для которой требуется, чтобы она управлялась и поддерживалась в рабочем состоянии *организацией* (3.50), и носитель, на котором она содержится

Примечание 1 к определению: Документированная информация может быть в любом формате, на любом носителе и из любого источника.

Примечание 2 к определению: Документированная информация может относиться к

- *системе менеджмента* (3.41), включая связанные с ней *процессы* (3.54);
- информации, созданной *организацией* (3.50) для обеспечения функционирования (документация);
- свидетельствам достигнутых результатов (записи).

3.20

результативность (effectiveness)

степень, с которой запланированные задачи выполнены и запланированные результаты достигнуты

3.21

событие (event)

возникновение или изменение определенного набора обстоятельств

Примечание 1 к определению: Событие может быть единичным или многократным и может иметь несколько причин.

Примечание 2 к определению: Событие может заключаться в том, что чего-то не случилось

Примечание 3 к определению: Событие может иногда обозначаться как «инцидент» или «происшествие»

[ИСТОЧНИК: ISO Guide 73:2009, 3.5.1.3, изменено – удалено Примечание 4 к определению]

3.22

внешний контекст (external context)

внешняя среда, в которой организация стремиться достичь своих *целей* (3.49)

Примечание 1 к определению: Внешний контекст может включать:

- культурную, социальную, политическую, юридическую, нормативную, финансовую, технологическую, экономическую, природную и конкурентную среду, на международном, национальном, региональном или местном уровне;
- ключевые движущие факторы и тенденции, оказывающие влияние на *цели организации* (3.50);
- взаимоотношения с внешними *заинтересованными сторонами* (3.37), их мнения и ценности.

[ИСТОЧНИК: ISO Guide 73:2009, 3.3.1.1]

3.23

управление информационной безопасностью (governance of information security)

система, посредством которой направляются и контролируются действия *организации* (3.50) в сфере *информационной безопасности* (3.28)

3.24

руководящий орган управления (governing body)

лицо или группа лиц, несущих ответственность за *показатели деятельности* (3.52) *организации* (3.50)и ее соответствие требованиям

Примечание 1 к определению: Руководящий орган управления может в некоторых юрисдикциях иметь форму совета директоров

3.25

индикатор (indicator)

показатель (3.42), который представляет собой прогнозную или вычисляемую оценку

3.26

информационная потребность в (information need)

осознаваемая необходимость управления *задачами* (3.49), целями, рисками и проблемами

[ИСТОЧНИК: ISO/IEC 15939:2017, 3.12]

3.27

средства обработки информации (information processing facilities)

любая система обработки информации, служба или инфраструктура, или физическое место их размещения

3.28

информационная безопасность (information security)

сохранение *конфиденциальности* (3.10), *целостности* (3.36) и *возможности применения* (3.7) информации

Примечание 1 к определению: Кроме того, могут быть использованы другие свойства, такие как *подлинность* (3.6), контролируемость, *неопровержимость авторства* (3.48) и *надежность* (3.55).

3.29

непрерывность информационной безопасности (information security continuity)

процессы (3.54) и процедуры, гарантирующие постоянное обеспечение *информационной безопасности* (3.28)

3.30

событие информационной безопасности (information security event)

установленное возникновение состояния системы, службы или сети, указывающее на возможное нарушение *информационной безопасности* (3.28), *политики* (3.53) или на сбой в работе *средств управления* (3.14), или на ранее неизвестную ситуацию, которая может иметь отношение к безопасности

3.31

инцидент информационной безопасности (information security incident)

одно или последовательность нежелательных или неожиданных *событий информационной безопасности* (3.30), которые со значительной степенью вероятности подвергают опасности деловую деятельность и угрожают *информационной безопасности* (3.28)

3.32

менеджмент инцидентов информационной безопасности (information security incident management)

совокупность *процессов* (3.54) для обнаружения, информирования, оценки, реагирования, обработки *инцидентов информационной безопасности* (3.31)и излечения уроков из них

3.33

профессионал системы менеджмента информационной безопасности (information security management system professional)

лицо, которое разрабатывает, внедряет, поддерживает в рабочем состоянии и осуществляет постоянное улучшение одного или нескольких *процессов* (3.54) системы менеджмента информационной безопасности

3.34

сообщество обмена информацией (information sharing community)

группа *организаций* (3.50), которые достигли соглашения о совместном использовании информации

Примечание 1 к определению: В качестве организации может выступать отдельное лицо

3.35

информационная система (information system)

совокупность приложений, служб, ИТ-активов или других компонентов обработки информации

3.36

целостность (integrity)

свойство сохранения полноты и точности

3.37

заинтересованная сторона (interested party)

stakeholder (допустимый термин)

лицо или *организация* (3.50), которые могут влиять на решения или действия, а также на которых могут влиять или они полагают, что на них могут влиять решения или действия

3.38

внутренний контекст (internal context)

внутренняя среда, в которой *организация* (3.50) стремится достичь решения своих задач

Примечание 1 к определению: Внутренний контекст может включать:

- органы управления, организационную структуру, роли и обязанности;
- *политики* (3.53), *задачи* (3.49) и стратегии, которые применяются для их достижения;
- возможности, понимаемые в терминах ресурсов и накопленных знаний (например, капитал, время, персонал, *процессы* (3.54), системы и технологии);
- *информационные системы* (3.35), информационные потоки и процессы принятия решений (как формализованные, так и не формализованные);
- отношения с внутренними *заинтересованными сторонами* (3.37), их мнения и ценности;
- корпоративная культура организации;
- стандарты, руководства и модели, принятые организацией;
- форму и объем договорных отношений.

[ИСТОЧНИК: ISO Guide 73:2009, 3.3.1.2]

3.39

уровень риска (level of risk)

величина *риска* (3.61), выраженная комбинацией *последствий* (3.12) и их *вероятности* (3.40)

[ИСТОЧНИК: ISO Guide 73:2009, 3.6.1.8, изменено – исключена из определения формулировка «или комбинация рисков»]

3.40

вероятность (likelihood)

возможность того, что что-то произойдет

[ИСТОЧНИК: ISO Guide 73:2009, 3.6.1.1, изменено – удалены Примечания 1 и 2 к определению]

3.41

система менеджмента (management system)

совокупность взаимосвязанных или взаимодействующих элементов *организации* (3.50) для разработки *политик* (3.53), *задач* (3.49) и *процессов* (3.54) для решения этих задач

Примечание 1 к определению: Система менеджмента может быть ориентирована на один или несколько объектов управления.

Примечание 2 к определению: К элементам системы менеджмента относятся структура организации, роли и ответственности, планирование и функционирование.

Примечание 3 к определению: Область действия системы менеджмента может включать всю организацию, отдельные и определенные функции организации, отдельные и определенные части организации, или одну или более сквозных функций, выполняемых в рамках группы организаций.

3.42

показатель (measure)

переменная, значение которой присваивается в результате *измерения* (3.43)

[ИСТОЧНИК: ISO/IEC 15939:2017, 3.15, изменено – удалено Примечание 2 к определению]

2.43

измерение (measurement)

процесс (3.54) определения значения

3.44

функция расчета производного показателя (measurement function)

алгоритм или расчет, выполняемый для объединения двух или более *основных показателей* (3.8)

[ИСТОЧНИК: ISO/IEC 15939:2017, 3.20]

3.45

метод измерения (measurement method)

логическая последовательность действий, описанная в общем виде, используемая для количественного определения атрибута относительно заданной шкалы

Примечание 1 к определению: Тип метода измерения зависит от характера операций, применяемых для количественного определения *атрибута* (3.4). Могут быть выделены два типа:

- субъективный: количественная оценка основывается на суждении человека; и
- объективный: количественная оценка основывается на числовых методах.

[ИСТОЧНИК: ISO/IEC 15939:2017, 2.21, изменено – удалено Примечание 2 к определению]

3.46

мониторинг (monitoring)

определение состояния системы, *процесса* (3.54) или задачи

Примечание 1 к определению: Для определения состояния может быть необходимым проверять, контролировать или критически наблюдать.

3.47

несоответствие (nonconformity)

невыполнение *требования* (3.56)

3.48

неопровержимость авторства (non-repudiation)

возможность доказать наступление оспариваемого *события* (3.21) или осуществление оспариваемого действия и инициировавших его источников

3.49

задача (objective)

результат, который должен быть достигнут

Примечание 1 к определению: Задача может быть стратегической, тактической или оперативной

Примечание 2 к определению: Задачи могут относиться к различным областям (таким как финансы, здоровье и безопасность, а также цели в области экологии) и могут задаваться на разных уровнях (например, стратегическом, всей организации, проекта, продукта и *процесса* (3.54)).

Примечание 3 к определению: Задача может быть выражена другими способами, например, как ожидаемый результат, целевое назначение, эксплуатационный критерий, как цель в области информационной безопасности или при помощи других слов с подобным значением (например, aim, goal или target). [последнее имеет смысл только для англоязычной версии – прим. пер.]

Примечание 4 к определению: В контексте систем менеджмента информационной безопасности задачи устанавливаются организацией в соответствии с политикой информационной безопасности для достижения определенных результатов.

3.50

организация (organization)

лицо или группа лиц, наделенные своими собственными функциями с обязанностями, полномочиями и взаимосвязями для решения своих *задач* (3.49)

Примечание 1 к определению: Понятие организации включает, но не ограничено этим, индивидуального предпринимателя, компанию, корпорацию, фирму, предприятие, орган власти, партнерство, благотворительную организацию или учреждение, часть или комбинацию всего перечисленного, имеющих или не имеющих статус юридического лица, государственных или частных.

3.51

передавать на аутсорсинг (outsource)

заключать соглашение, по которому внешняя *организация* (3.50) выполняет часть функций или *процесса* (3.54) организации

Примечание 1 к определению: Внешняя организация находится вне области действия *системы менеджмента* (2.46), хотя передаваемая на аутсорсинг функция или *процесс* (2.61) входят в эту область.

3.52

показатель деятельности (performance)

измеримый результат

Примечание 1 к определению: Показатель деятельности может быть связан как с количественными, так и качественными результатами.

Примечание 2 к определению: Показатель деятельности может относиться к управлению работами, *процессами* (3.54), продуктами (включая услуги), системами или *организациями* (3.50).

3.53

политика (policy)

намерения и направление развития *организации* (3.50), официально сформулированные *высшим руководством* (3.75)

3.54

процесс (process)

совокупность взаимосвязанных или взаимодействующих видов деятельности, которая преобразует входы в выходы

3.55

надежность (reliability)

свойство соответствия предполагаемому поведению и результатам

3.56

требование (requirement)

потребность или ожидание, которое установлено, подразумевается по умолчанию или является обязательным

Примечание 1 к определению: "Подразумеваемая по умолчанию" означает, что это обычная или общепринятая практика для организации и заинтересованных сторон, когда рассматриваемые потребности или ожидания предполагаются.

Примечание 2 к определению: Установленным требованием является такое требование, которое определено, например, в документированной информации.

3.57

остаточный риск (residual risk)

риск (3.61), оставшийся после *обработки риска* (3.72)

Примечание 1 к определению: Остаточный риск может заключать в себе не выявленный риск.

Примечание 2 к определению: Остаточный риск может также называться «сохраняющимся риском»

3.58

анализ (review)

деятельность, предпринимаемая для определения пригодности, адекватности и *результативности* (3.20) объекта анализа с точки зрения решения установленных *задач* (3.49)

[ИСТОЧНИК: ISO Guide 73:2009, 3.8.2.2, изменено – удалено Примечание 1 к определению]

3.59

объект анализа (review object)

конкретный объект, подвергаемый анализу

3.60

цель анализа (review objective)

описание того, что должно быть достигнуто в результате *анализа* (3.59)

3.61

риск (risk)

влияние неопределенности на *цели* (3.49)

Примечание 1 к определению: Влияние – это отклонение от ожидаемого – положительное или отрицательное.

Примечание 2 к определению: Неопределенность – состояние хотя бы частичной нехватки информации, связанной с пониманием события или знанием о нем, его последствий или вероятности.

Примечание 3 к определению: Риск часто характеризуется ссылкой на возможные «события» (как это определено в ISO Guide 73:2009, 3.5.1.3) и «последствия» (как это определено в ISO Guide 73:2009, 3.6.1.3), или их комбинации.

Примечание 4 к определению: Риск часто выражается в форме комбинации последствий события (включая изменения в обстоятельствах) и связанной с ним «вероятности» (как это определено в ISO Guide 73:2009, 3.6.1.1) возникновения.

Примечание 5 к определению: В контексте систем менеджмента информационной безопасности, риски могут быть выражены как влияние неопределенности на задачи в области информационной безопасности.

Примечание 6 к определению: риск в сфере информационной безопасности связан с возможностью того, что угрозы будут реализовываться через использование уязвимостей информационного актива или группы информационных активов и, тем самым, наносить ущерб организации.

3.62

принятие риска (risk acceptance)

обоснованное решение согласиться с конкретным *риском* (3.61)

Примечание 1 к определению: Принятие риска может происходить без *обработки риска* (3.72) или в *процессе* (3.54) обработки риска.

Примечание 2 к определению: Принятые риски подлежат *мониторингу* (3.46) и *анализу* (3.58).

[ИСТОЧНИК: ISO Guide 73:2009, 3.7.1.6]

3.63

анализ риска (risk analysis)

процесс (3.54) понимания характера *риска* (3.61) и определения *уровня риска* (3.39)

Примечание 1 к определению: Анализ риска обеспечивает основу для *определения степени риска* (3.67) и принятия решения об *обработке риска* (3.72).

Примечание 2 к определению: Анализ рисков включает прогнозную оценку риска.

[ИСТОЧНИК: ISO Guide 73:2009, 3.6.1]

3.64

оценка риска (risk assessment)

единый *процесс* (3.54) *идентификации риска* (3.68), *анализа риска* (3.63) и *определения степени риска* (3.67).

[ИСТОЧНИК: ISO Guide 73:2009, 3.4.1]

3.65

обмен информацией по рискам и консультации (risk communication and consultation)

совокупность непрерывных и повторяющихся *процессов* (3.54), выполняемых организацией для передачи, совместного использования или получения информации и

участия в диалоге с *заинтересованными сторонами* (3.37) по вопросам менеджмента *риска* (2.61).

Примечание 1 к определению: Информация может относиться к наличию, характеру, форме, *вероятности* (3.41), значимости, оцениванию, приемлемости риска и его обработке.

Примечание 2 к определению: Консультации являются двусторонним процессом содержательного обмена информацией между *организацией* (3.50) и заинтересованными сторонами по какому-либо вопросу до принятия решения или определения направления действий по этому вопросу. Консультация – это:

- *процесс*, который воздействует на принятие решения посредством влияния, а не власти; и
- предварительный этап принятия решения, а не совместное принятие решения.

3.66

критерий риска (risk criteria)

эталонные условия, в сравнении с которыми оценивают значимость *риска* (3.61)

Примечание 1 к определению: Критерии риска базируются на целях организации, *внешнем* (3.22) и *внутреннем контексте* (3.38).

Примечание 2 к определению: Критерии риска могут быть сформированы на основе стандартов, законодательных актов, *политик* (3.53) и иных *требований* (3.56).

[ИСТОЧНИК: ISO Guide 73:2009, 3.3.1.3]

3.67

определение степени риска (risk evaluation)

процесс (3.54) сравнения результатов *анализа риска* (3.63) с *критериями риска* (*3.66*) для определения, является ли *риск* (3.61) и/или его величина допустимыми или приемлемыми

Примечание 1 к определению: Определение степени риска помогает при принятии решения об *обработке риска* (3.72)

[ИСТОЧНИК: ISO Guide 73:2009, 3.7.1]

3.68

идентификация риска (risk identification)

процесс (3.54) поиска, распознавания и описания *рисков* (3.61)

Примечание 1 к определению: Идентификация риска может включать в себя выявление источников риска, *событий* (3.21), их причин и возможных *последствий* (3.12).

Примечание 2 к определению: При идентификации риска могут использоваться данные за прошедший период, аналитические методы, обоснованные мнения и экспертные оценки, а также потребности *заинтересованных сторон* (3.37).

[ИСТОЧНИК: ISO Guide 73:2009, 3.5.1]

3.69

менеджмент риска (risk management)

скоординированные действия по руководству и управлению *организацией* (3.50) в отношении *рисков* (3.61)

[ИСТОЧНИК: ISO Guide 73:2009, 2.1]

3.70

процесс менеджмента риска (risk management process)

систематическое применение управленческих *политик* (3.53), процедур и установленных методик к действиям по обмену информацией, консультациям, установлению контекста, а также идентификации, анализу, определению степени, обработке, мониторингу и повторному анализу *риска* (3.61)

Примечание 1 к определению: ISO/IEC 27005 использует термин «*процесс*» (3.54) для описания менеджмента риска в целом. Элементы процесса *менеджмента риска* (3.69) там обозначены термином «действия» («activities»).

[ИСТОЧНИК: ISO Guide 73:2009, 3.1, изменено – добавлено Примечание 1 к определению]

3.71

владелец риска (risk owner)

лицо или организация, обладающие ответственностью и полномочиями для менеджмента *риска* (3.61)

[ИСТОЧНИК: ISO Guide 73:2009, 3.5.1.5]

3.72

обработка риска (risk treatment)

процесс (3.54), нацеленный на изменение *риска* (3.61)

Примечание 1 к определению: Обработка риска может включать в себя:

- избегание риска путем принятия решения не начинать или не продолжать деятельность, которая приводит к возникновению риска;
- принятие или повышение степени риска с целью реализации возможностей;
- устранение источника риска;
- изменение *вероятности* (3.40);
- изменение *последствий* (3.12);
- разделение риска с другой стороной или сторонами (путем включения в контракты или финансового обеспечения риска);
- сохранение риска на основе обоснованного выбора.

Примечание 2 к определению: Меры по обработке риска, которые принимаются в отношении негативных последствий, иногда называются «снижением риска», «устранением риска» и «предотвращением риска».

Примечание 3 к определению: Обработка риска может создавать новые риски и изменять существующие.

[ИСТОЧНИК: ISO Guide 73:2009, 3.8.1, изменено – в Примечании 1 к определению слово «решение» заменено на «выбор»]

3.73

стандарт обеспечения безопасности (security implementation standard)

документ, устанавливающий разрешенные методы обеспечения безопасности

3.74

угроза (threat)

возможная причина нежелательного инцидента, который может нанести ущерб системе или *организации* (3.50)

3.75

высшее руководство (top management)

лицо или группа лиц, которая направляет и управляет *организацией* (3.50) на высшем уровне

Примечание 1 к определению: Высшее руководство обладает правом делегировать полномочия и обеспечивать ресурсами в пределах организации.

Примечание 2 к определению: Если область действия *системы менеджмента* (3.41) охватывает только часть организации, тогда термин «высшее руководство» относится к тем, кто управляет этой частью организации.

Примечание 3 к определению: Высшее руководство иногда называется исполнительным руководством и может включать в себя руководителя организации (CEO), финансового директора (CFO), директора по ИТ (CIO) и подобные должности.

3.76

доверенный участник информационного сообщества (trusted information communication entity)

автономная *организация* (3.50), поддерживающая информационное взаимодействие в

рамках *сообщества обмена информацией* (3.34)

3.77

уязвимость (vulnerability)

слабое место актива или *средства управления* (3.14), через которое может реализоваться одна или более *угроза* (3.74)

4 Системы менеджмента информационной безопасности

4.1 Общие положения

Организации всех типов и размеров:

a) собирают, обрабатывают, хранят и передают информацию;

b) осознают, что информация и связанные с ней процессы, системы, сети и персонал являются важными активами для достижения целей организации;

c) сталкиваются с рядом рисков, которые могут влиять на функционирование активов; и

d) принимают меры в отношении предполагаемого воздействия рисков, внедряя средства управления информационной безопасностью.

Вся информация, обращающаяся в организации и обрабатываемая ею, подвергается угрозам атак, ошибок, негативных природных явлений (например, наводнение или пожар), и т.д., а также является объектом влияния уязвимостей, сопряженных с использованием информации. Концепция информационной безопасности в своей основе рассматривает информацию как актив, который представляет ценность, требующую соответствующей защиты, например, от потери возможности применения, конфиденциальности и целостности. Обеспечение возможности своевременного использования точной и полной информации тому, у кого есть соответствующие потребности, способствует эффективности бизнеса.

Защита информационных активов за счет результативного определения, достижения, обеспечения и улучшения информационной безопасности является существенной для способности организации достигать своих целей, а также поддержания и улучшения соответствия законодательным требованиям и имиджа. Эти скоординированные действия, направляющие выполнение соответствующих средств управления и обрабатывающие признанные неприемлемыми информационные риски, широко известны как элементы менеджмента информационной безопасности.

В связи с тем, что риски информационной безопасности и результативность средств управления меняются в зависимости от изменяющихся обстоятельств, организации необходимо:

a) отслеживать и оценивать результативность осуществляемых средств управления и процедур;

b) выявлять появляющиеся риски, которые должны быть обработаны; и

c) выбирать, выполнять и улучшать соответствующие средства управления по мере необходимости.

Чтобы обеспечить взаимосвязь и координацию таких действий по информационной безопасности, каждой организации необходимо разработать политику и цели в области информационной безопасности и результативно достигать этих целей за счет применения системы менеджмента.

4.2 Что такое СМИБ?

4.2.1 Общий обзор и принципы

Система менеджмента информационной безопасности (СМИБ) включает в себя политики, процедуры, руководства и соответствующие ресурсы и задачи, коллегиально управляемые организацией в целях защиты ее информационных активов. СМИБ представляет собой системный подход к разработке, внедрению, функционированию, мониторингу, анализу, обеспечению и улучшению информационной безопасности организации для достижения бизнес-целей. Она основывается на оценке рисков и уровнях приемлемости рисков организации, установленных таким образом, чтобы результативно обрабатывать риски и управлять ими. Анализ требований к защите информационных активов и применению средств управления для обеспечения защиты этих информационных активов в соответствии с ситуацией, вносит свой вклад в успешную реализацию СМИБ. Следующие фундаментальные принципы также способствуют успешной реализации СМИБ:

a) осознание необходимости обеспечения информационной безопасности;

b) назначение ответственности за информационную безопасность;

c) увязывание обязательств руководства с интересами заинтересованных сторон;

d) повышение значения социальных ценностей;

e) оценка риска, определяющая соответствующие средства управления для обеспечения приемлемых уровней риска;

f) безопасность, как неотъемлемый элемент информационных сетей и систем;

g) активное предупреждение и выявление инцидентов информационной безопасности;

h) обеспечение комплексного подхода к управлению информационной безопасностью;

i) постоянная переоценка уровня информационной безопасности и внесение изменений при необходимости.

4.2.2 Информация

Информация – это актив, который, подобно другим важным активам, является существенным для бизнеса организации и, следовательно, должен быть соответствующим образом защищен. Информация может сохраняться в различных формах, в том числе: цифровой (например, файлы, хранящиеся на электронных или оптических носителях), на материальных носителях (например, бумаге), а также скрытой - в форме знаний сотрудников. Информация может передаваться различными средствами, включая: курьеров, электронные и голосовые средства связи. Какая бы форма или какие бы средства не использовались для передачи информации, она всегда должна быть соответствующим образом защищена.

Во многих организациях информация зависит от информационно-коммуникационных технологий. Эти технологии зачастую – существенный элемент в организации, который облегчает создание, обработку, хранение, передачу, защиту и утилизацию информации.

4.2.3 Информационная безопасность

Информационная безопасность гарантирует конфиденциальность, возможность применения и целостность информации. Информационная безопасность предполагает применение и управление соответствующими средствами обеспечения безопасности, которые учитывают широкий диапазон угроз с целью гарантировать устойчивый успех бизнеса и минимизировать влияние инцидентов информационной безопасности.

Информационная безопасность достигается посредством выполнения соответствующего набора средств управления, сформированного в ходе выбранного процесса менеджмента

риска и управляемого посредством СМИБ, включая политики, процессы, процедуры, организационные структуры, программное и техническое обеспечение для защиты определенных информационных активов. Эти средства управления должны быть определены, внедрены, контролироваться, анализироваться и улучшаться, если необходимо, чтобы гарантировать достижение установленного уровня информационной безопасности и бизнес-целей. Ожидается, что соответствующие средства управления информационной безопасности будут встроены в бизнес-процессы организации.

4.2.4 Менеджмент

Менеджмент включает в себя деятельность по руководству, контролю и постоянному улучшению организации в рамках соответствующих структур. Менеджмент предполагает действие, способ или принятый порядок организации, управления и контроля ресурсов. Структура управления может состоять из одного человека в небольшой организации и до целой управленческой иерархии, в которую включены многие люди, в больших организациях.

В терминах СМИБ менеджмент подразумевает руководство и принятие решений, необходимых для достижения бизнес-целей, направленных на защиту информационных активов организации. Менеджмент информационной безопасности реализуется через формулирование и применение политик, процедур и руководств по информационной безопасности, которые затем применяются во всей организации всеми, кто связан с этой организацией.

4.2.5 Система менеджмента

Система менеджмента использует ресурсы для достижения целей организации. Система менеджмента включает в себя организационную структуру, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы.

С точки зрения информационной безопасности система менеджмента позволяет организации:

a) удовлетворять требования потребителей и других заинтересованных сторон к информационной безопасности;

b) совершенствовать планы и деятельность организации;

c) достигать целей организации в области информационной безопасности;

d) соответствовать нормативным, законодательным и отраслевым требованиям; и

e) управлять информационными активами системным образом, что способствует постоянному улучшению и согласованности с текущими целями организации.

4.3 Процессный подход

Организациям необходимо выделять и управлять многими видами деятельности для того, чтобы функционировать результативно и эффективно. Любая деятельность, использующая ресурсы, должна управляться, чтобы обеспечить преобразование входов в выходы выполнением совокупности взаимосвязанных и взаимодействующих видов деятельности, которая также известна как процесс. Выход одного процесса может непосредственно быть входом другого процесса и, как правило, рассматриваемое преобразование происходит в планируемых и контролируемых условиях. Применение системы процессов в организации наряду с выделением и взаимодействием этих процессов, а также управление ими, может называться «процессным подходом».

4.4 Почему СМИБ – это важно

Риски, связанные с информационными активами организации, должны быть обработаны. Обеспечение информационной безопасности требует управления рисками и охватывает

риски, связанные с физическими и технологическими угрозами и угрозами, порождаемыми человеческим фактором, в отношении всех форм информации, обращающейся или используемой в организации.

Предполагается, что выбор в пользу СМИБ должен быть стратегическим решением для организации и необходимо, чтобы это решение органично сочеталось, соизмерялось и изменялось в соответствии с потребностями организации.

Проектирование и внедрение СМИБ организации зависит от потребностей и целей организации, требований безопасности, осуществляемых бизнес-процессов, размера и структуры организации. Разработка и функционирование СМИБ должны отражать интересы и требования информационной безопасности всех заинтересованных сторон организации, включая потребителей, поставщиков, партнеров по бизнесу, акционеров и прочих соответствующих третьих сторон.

Во взаимосвязанном мире информация и связанные с ней процессы, системы и сети образуют критически важные для бизнеса активы. Организации и их информационные системы и сети подвергаются угрозам безопасности из широкого ряда источников, включая мошенничество с использованием компьютеров, шпионаж, саботаж, вандализм, пожар и наводнение. Ущерб информационным системам и сетям наносится и посредством вредоносного кода, взлома компьютеров, а также DDoS атак, которые становятся все более распространенными, масштабными и изощренными.

СМИБ важна как в государственном секторе, так и в частном бизнесе. В любой отрасли СМИБ является инструментом, который поддерживает электронный бизнес, и является существенной для управления рисками. Взаимные связи общедоступных и частных сетей и совместное использование информационных активов увеличивают сложность контроля доступа к информации и ее обработки. Кроме того, распространение переносных устройств хранения, содержащих информационные активы, может снизить результативность традиционных средств управления. Принимая требования семейства стандартов СМИБ, организации могут продемонстрировать бизнес-партнерам и другим заинтересованным сторонам свою способность применять согласованные и взаимно признаваемые принципы информационной безопасности.

Информационная безопасность не всегда принимается во внимание при проектировании и разработке информационных систем. К тому же, информационная безопасность часто воспринимается как чисто техническое решение. Однако, уровень информационной безопасности, который может быть обеспечен только техническими средствами, ограничен и может быть нерезультативным без поддержки соответствующего менеджмента и процедур в рамках СМИБ. Встраивание безопасности в функционально завершенную систему может быть трудным и затратным делом. СМИБ предполагает определение, какие средства управления уже внедрены, и требует тщательного планирования и внимания к деталям. Как пример, средства управления доступом, которые могут быть техническими (логическими), физическими, административными (управленческими) или их комбинацией, обеспечивают методы, гарантирующие, что доступ к информационным активам является разрешенным и предоставляется в соответствии с ограничениями, вытекающими из требований бизнеса и информационной безопасности.

Успешное применение СМИБ является важным для защиты информационных активов, позволяя организации:

a) достигать большей уверенности, что ее информационные активы соответствующим образом постоянно защищены от угроз;

b) поддерживать структурированную и всеохватывающую систему для выявления и оценки рисков информационной безопасности, выбора и применения

соответствующих средств управления, а также измерения и улучшения их результативности;

c) постоянно улучшать среду управления; и

d) результативно обеспечивать соответствие законодательным и нормативным требованиям.

4.5 Разработка, мониторинг, обеспечение и улучшение СМИБ

4.5.1 Общий обзор

Организации необходимо предпринимать следующие шаги при разработке, мониторинге, обеспечении функционирования и улучшении СМИБ:

a) определить информационные активы и связанные с ними требования информационной безопасности (см. 4.5.2);

b) оценить риски информационной безопасности (см. 4.5.3) и обработать риски информационной безопасности (см. 4.5.4);

c) выбрать и внедрить соответствующие средства управления в отношении неприемлемых рисков (см. 4.5.5);

d) контролировать, поддерживать и улучшать результативность средств управления, связанных с информационными активами организации (см. 4.5.6).

Чтобы гарантировать, что СМИБ результативно и непрерывно защищает информационные активы организации, необходимо постоянно повторять шаги (a) – (d) для выявления изменений в рисках или стратегии организации, или целях бизнеса.

4.5.2 Определение требований информационной безопасности

В рамках общей стратегии и бизнес-целей организации, с учетом ее размера и географического расположения, требования информационной безопасности могут быть определены на основе понимания:

a) выявленных информационных активов и их ценности;

b) потребностей бизнеса в обработке, хранении и обмене информацией;

c) законодательных, нормативных и контрактных требований.

Проведение систематической оценки рисков, связанных с информационными активами организации, включает в себя анализ угроз информационным активам, уязвимостей и вероятности реализации угроз информационным активам, а также потенциального влияния любого инцидента информационной безопасности на информационные активы. Предполагается, что затраты на соответствующие средства управления должны быть пропорциональны предполагаемому воздействию на бизнес при реализации рисков.

4.5.3 Оценка рисков информационной безопасности

Управление рисками информационной безопасности требует соответствующей оценки рисков и метода обработки рисков, которые могут включать оценку потерь и выгод, законодательные требования, вопросы, вызывающие озабоченность заинтересованных лиц и другие соответствующие исходные данные.

В ходе оценки рисков следует выявлять, количественно оценивать и выстраивать риски по приоритетам в соответствии с критериями приемлемости рисков и целями, существенными для организации. Эти результаты должны служить ориентиром и определять соответствующие управленческие действия и приоритеты для управления рисками информационной безопасности и внедрения средств управления, выбранных для защиты от этих рисков.

Оценка рисков должна включать:

- систематический подход к оценке величины риска (анализ риска); и
- процесс сравнения прогнозной оценки риска с критериями для определения значимости рисков (определение степени риска).

Оценку рисков следует выполнять периодически для учета изменений в требованиях информационной безопасности и ситуации с рисками, связанными, например, с активами, угрозами, уязвимостями, воздействиями, оценкой степени риска, а также когда происходят существенные изменения. Такая оценка рисков должна иметь систематический характер, обеспечивая получение сравнимых и воспроизводимых результатов.

Оценка информационных рисков, для того, чтобы быть результативной, должна иметь четко определенную область применения и включать связи с оценкой рисков в других областях, если необходимо.

ISO/IEC 27005 содержит рекомендации по менеджменту рисков информационной безопасности, включая советы по оценке рисков, обработке рисков, принятию рисков, отчетах о рисках, мониторингу и анализу рисков. Там же приведены и примеры методологий оценки рисков.

4.5.4 Обработка рисков информационной безопасности

До того, как рассматривать средства обработки рисков, организации следует принять критерии оценки, позволяющие определить, является ли риск приемлемым или нет. Риски могут быть приемлемыми если, например, в результате оценки они признаны низкими или затраты на обработку экономически неоправданы для организации. Такие решения должны быть оформлены документально.

Для каждого риска, выявленного в результате оценки, должно быть принято решение по обработке этого риска. Возможные варианты обработки риска включают в себя:

a) применение соответствующих средств управления для снижения рисков;

b) осознанное и объективное принятие рисков, обеспечивающее их уровень, который полностью удовлетворяет политике организации и критериям приемлемости риска;

c) избежание рисков за счет исключения действий, которые могли бы привести к возникновению рисков;

d) разделение рисков с другими сторонами, например, страховщиками или поставщиками.

Для тех рисков, по которым было принято решение о применении для их обработки соответствующих средств управления, эти средства управления должны быть выбраны и внедрены.

4.5.5 Выбор и внедрение средств управления

После того, как установлены требования информационной безопасности (см. 4.5.2), определены и оценены риски информационной безопасности для выявленных информационных активов (см. 4.5.3), а также приняты решения по обработке рисков информационной безопасности (см. 4.5.4), выполняется выбор и внедрение средств управления для снижения рисков.

Средства управления должны гарантировать, что риски снижаются до приемлемого уровня с учетом следующего:

a) требований и ограничений национального и международного законодательства и нормативных актов;

b) целей организации;

c) эксплуатационных требований и ограничений;

d) затрат на их внедрение и выполнение в отношении тех рисков, которые должны быть снижены, и сохранение их пропорциональности требованиям и ограничениям организации;

e) их задач в части мониторинга, оценки и улучшения эффективности и результативности средств управления информационной безопасностью для обеспечения достижения целей организации. Выбор и внедрение средств управления должны быть документированы в рамках заявления о применимости для способствования выполнению требований;

f) необходимости соблюдения баланса между затратами на внедрение и выполнение средств управления и возможными потерями от инцидентов информационной безопасности.

Средства управления, представленные в ISO/IEC 27002, признаны лучшими практиками, применимыми в большинстве организаций и легко адаптируемыми к организациям различного размера и сложности. Другие стандарты семейства содержат рекомендации по выбору и применению средств управления СМИБ, представленных в ISO/IEC 27002.

Средства управления информационной безопасностью должны учитываться на стадии разработки системных и проектных технических заданий и на стадии проектирования. Пренебрежение этим может вести к дополнительных затратам и снижению результативности решений, и, возможно, в худшем случае, к неспособности обеспечить надлежащую безопасность. Средства управления могут быть выбраны из числа предлагаемых ISO/IEC 27002 или из иного набора средств. Кроме того, могут быть разработаны новые средства управления для под конкретные потребности организации. Необходимо понимать, что некоторые средства управления могут и не подходить всем информационным системам и средам, и не быть применимыми на практике для всех организаций.

Иногда требуется время, чтобы внедрить выбранный набор средств управления, и в течение этого периода времени уровень риска может быть выше, чем он должен быть в долгосрочной перспективе. Критерии риска должны устанавливаться для уровня приемлемости рисков на краткосрочную перспективу, пока внедряются средства управления. Заинтересованные стороны должны информироваться об уровне ожидаемого риска в разные моменты времени, пока внедряются средства управления.

Следует помнить, что нет такого набора средств управления, который мог бы обеспечить полную безопасность. Должны предприниматься дополнительные управляющие действия для мониторинга, оценки и улучшения эффективности и результативности средств управления информационной безопасностью для обеспечения достижения целей организации.

Выбор и внедрение средств управления должны быть документированы в рамках заявления о применимости, чтобы способствовать выполнению требований. [повтор положения из пункта «e» – прим. пер.]

4.5.6 Мониторинг, обеспечение и улучшение результативности СМИБ

Организации необходимо обеспечивать работоспособность и улучшать СМИБ посредством мониторинга и оценки функционирования в соответствии с политиками и целями организации, а также передачи руководству данных о результатах для проведения анализа. Такой анализ СМИБ должен установить, содержит ли система конкретные средства управления, которые подходят для обработки рисков в рамках области действия СМИБ. Кроме того, на основе записей, относящихся к отслеживаемой области, он обеспечит свидетельства проверки соответствия, а также прослеживаемость корректирующих, предупреждающих действий и действий по улучшению.

4.5.7 Постоянное улучшение

Цель постоянного улучшения СМИБ состоит в повышении вероятности достичь целей, связанных с сохранением конфиденциальности, возможности применения и целостности информации. Акцент при постоянном улучшении делается на изыскание возможностей для совершенствования, а не признании существующего управления достаточно хорошим или столь хорошим, насколько оно только может быть.

Действия по улучшению включают в себя следующее:

a) анализ и оценку существующей ситуации для определения областей улучшения;

b) установление целей улучшения;

c) поиск возможных решений для достижения этих целей;

d) оценку этих решений и осуществление выбора;

e) выполнение выбранных решений;

f) измерение, проверку, анализ и оценку результатов выполнения для определения, достигнуты ли поставленные цели;

g) формализованную фиксацию изменений.

Результаты анализируются, если необходимо, для определения дальнейших возможностей улучшения. Таким образом улучшение представляет собой постоянную деятельность, т.е. действия, которые часто повторяются. Обратная связь от потребителей и других заинтересованных сторон, данные аудитов и анализа системы менеджмента информационной безопасности также могут быть использованы для выявления возможностей улучшения.

4.6 Критические факторы успеха СМИБ

Большое число факторов является критическими для успешного функционирования СМИБ, позволяющего организации достичь своих бизнес-целей. Примеры таких критических факторов успеха включают в себя:

a) политику и задачи в области информационной безопасности и действия, согласованные с этими задачами;

b) подход и общие принципы для проектирования, внедрения, мониторинга, обеспечения и улучшения информационной безопасности, согласованные с корпоративной культурой;

c) видимую поддержку и обязательства на всех уровнях управления, особенно на высшем уровне;

d) понимание требований по защите информационных активов, достигаемое применением менеджмента рисков информационной безопасности (см. ISO/IEC 27005);

e) действенное ознакомление с информационной безопасностью, подготовку и обучающую программу, информирующую всех сотрудников и другие соответствующие стороны об обязательствах в отношении информационной безопасности, которые сформулированы в политиках информационной безопасности, стандартах и т.д., а также их мотивирование поступать надлежащим образом;

f) результативный процесс менеджмента инцидентами информационной безопасности;

g) действенный подход к менеджменту непрерывности бизнеса;

h) система измерений, используемая для оценки показателей деятельности в менеджменте информационной безопасности и предложения по улучшению, полученные по каналам обратной связи.

СМИБ увеличивает вероятность того, что организация будет постоянно обеспечивать критические факторы успеха, требуемые для защиты ее информационных активов.

4.7 Выгоды, получаемые от применения семейства стандартов на СМИБ

Преимущества от внедрения СМИБ будут, в первую очередь, выражены в снижении рисков информационной безопасности (т.е. снижении вероятности и/или ущерба от инцидентов информационной безопасности). Конкретно, преимущества, получаемые организацией в рамках достижения устойчивого успеха от внедрения семейства стандартов на СМИБ, включают в себя:

a) структурированную среду, поддерживающую процесс определения, внедрения, функционирования и обеспечения комплексной, эффективной, создающей ценность, интегрированной и согласованной СМИБ, которая соответствует потребностям организации, охватывая различные операции и участки;

b) помощь руководству в согласованном управлении и ответственном применении их подхода к менеджменту информационной безопасности в контексте корпоративного менеджмента рисков и управления, включая обучение и подготовку владельцев бизнеса и систем к комплексному управлению информационной безопасностью;

c) продвижение общепринятых в мировом масштабе практик по информационной безопасности в не директивной манере, давая организациям свободу применять и улучшать соответствующие средства управления, которые подходят к конкретным обстоятельствам, и поддерживать эти практики в условиях внутренних и внешних изменений;

d) обеспечение единой терминологии и понятийной основы для информационной безопасности, облегчающих установление доверия между деловыми партнерами при наличии СМИБ, соответствующей требованиям, особенно, если партнеры требуют сертификации по ISO/IEC 27001 аккредитованным органом по сертификации;

e) возрастание доверия заинтересованных сторон к организации;

f) удовлетворение социальных нужд и ожиданий;

g) более действенное управление инвестициями в информационную безопасность.

5 Семейство стандартов на СМИБ

5.1 4.1 Общая информация

Семейство стандартов СМИБ состоит из взаимосвязанных стандартов, как уже опубликованных, так и находящихся в разработке, и содержит несколько важных структурных компонентов. Эти компоненты сфокусированы на:

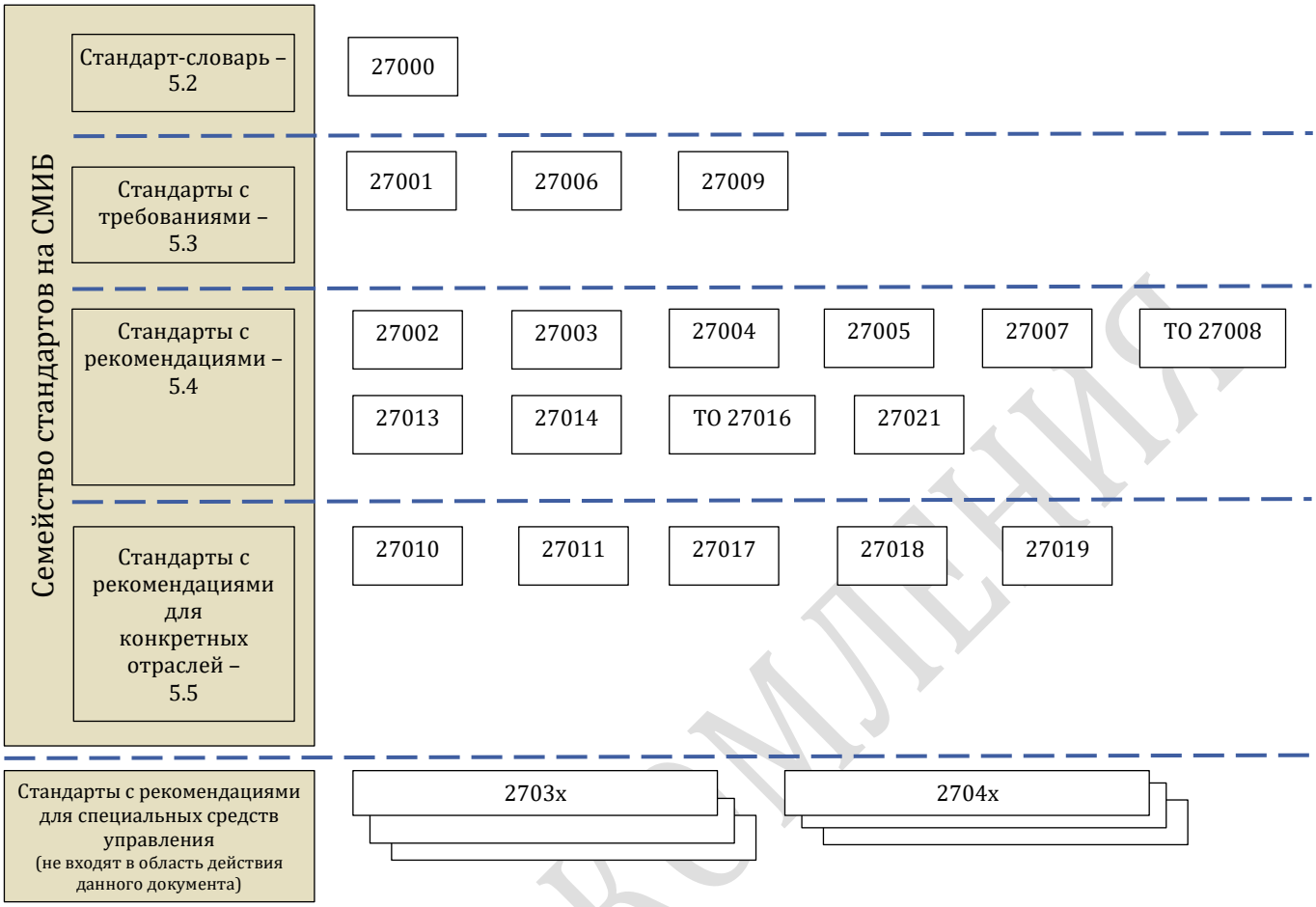
- стандартах, описывающих требования СМИБ (ISO/IEC 27001);
- требования к органам по сертификации (ISO/IEC 27006);
- дополнительные требования для внедрения СМИБ в конкретных отраслях (ISO/IEC 27009).

Другие документы содержат рекомендации по различным аспектам внедрения СМИБ, описывая общий процесс, а также рекомендации для конкретных отраслей.

Взаимосвязь между стандартами семейства показана на рис. 1.

Каждый из стандартов семейства определен ниже по его типу (или роли) в рамках семейства и его ссылочным номером.

Рисунок 1 - Взаимосвязи стандартов семейства СМИБ



5.2 Стандарт, описывающий общие принципы и терминологию: ISO/IEC 27000 (Данный документ)

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

Информационные технологии - Методы и средства обеспечения безопасности - Системы менеджмента информационной безопасности – Общие сведения и словарь

Область применения: Данный документ представляет организациям и отдельным лицам:

a) обзор семейства стандартов на СМИБ;

b) введение в системы менеджмента информационной безопасности; и

c) термины и определения, используемые во всех стандартах семейства.

Назначение: ISO/IEC 27000 описывает основы систем менеджмента информационной безопасности, которые составляют предмет семейства стандартов, а также определяет соответствующие термины.

5.3 Стандарты, устанавливающие требования

5.3.1 ISO/IEC 27001

Information technology — Security techniques — Information security management systems — Requirements

Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования

Область применения: Данный документ устанавливает требования к разработке,

внедрению, функционированию, мониторингу, анализу, обеспечению и улучшению формализованной системы менеджмента информационной безопасности (СМИБ) в контексте всех бизнес-рисков организации. Он устанавливает требования к применению средств управления информационной безопасностью, адаптированных под нужды каждой организации или каких-то ее частей. Данный документ может быть использован всеми организациями вне зависимости от типа, размера и характера бизнеса.

Назначение: ISO/IEC 27001 содержит нормативные требования к разработке и функционированию СМИБ, включая набор средств для управления рисками и их снижения, связанных с информационными активами, которые организация хотела бы защитить применением СМИБ. Организации, внедрившие СМИБ, могут подтверждать ее соответствие аудитами и сертификацией. В рамках данного процесса должны быть выбраны по ситуации соответствующие задачи и средства управления из Приложения А (ISO/IEC 27001 СМИБ), чтобы охватить выбранные требования. Задачи управления и средства управления, приведенные в таблице А.1 (ISO/IEC 27001) взяты непосредственно и полностью соответствуют тем, что приведены в разделах 5 – 18 ISO/IEC 27002.

5.3.2 ISO/IEC 27006

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Информационная технология – Методы и средства обеспечения безопасности – Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

Область применения: Данный документ устанавливает требования – в дополнение к требованиям, содержащимся в ISO/IEC 17021 – и дает рекомендации органам, проводящим аудиты и сертификацию СМИБ на соответствие ISO/IEC 27001. Он, в первую очередь, предназначен для обеспечения аккредитации органов по сертификации, проводящих сертификацию на соответствие ISO/IEC 27001.

Выполнение требований, содержащихся в данном документе, должно быть продемонстрировано в части компетентности и надежности любым лицом, проводящим сертификацию СМИБ, а руководящие указания, содержащиеся в данном документе, обеспечивают дополнительную интерпретацию этих требований для любого лица, проводящего сертификацию СМИБ.

Назначение: ISO/IEC 27006 дополняет ISO/IEC 17021 в части требований по аккредитации органов по сертификации, позволяя, таким образом, этим организациям выдавать сертификаты соответствия требованиям, установленным в ISO/IEC 27001.

5.3.3 ISO/IEC 27009

Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

Информационная технология – Методы и средства обеспечения безопасности – Применение ISO/IEC 27001 в конкретных отраслях – Требования

Область применения: Данный документ устанавливает требования для применения ISO/IEC 27001 в конкретных отраслях (сфере деятельности, области применения или секторе рынка). Он поясняет, каким образом ввести требования, дополнительные к тем, что содержатся в ISO/IEC 27001, как уточнить любые требования ISO/IEC 27001 и как добавить средства управления или комплекс средств управления в дополнение к тем, что содержатся в Приложении А стандарта ISO/IEC 27001:2013.

Назначение: ISO/IEC 27009 обеспечивает отсутствие конфликта между дополнительными или уточненными требованиями и требованиями ISO/IEC 27001.

5.4 Стандарты, содержащие общие рекомендации

5.4.1 ISO/IEC 27002

Information technology — Security techniques — Code of practice for information security controls

Информационная технология – Методы и средства обеспечения безопасности – Свод норм и правил менеджмента информационной безопасности

Область применения: Данный документ содержит перечень общепринятых задач управления и признанных наилучшими средств управления, которые должны использоваться как руководство при выборе и внедрении средств управления для обеспечения информационной безопасности.

Назначение: ISO/IEC 27002 содержит рекомендации по внедрению средств управления информационной безопасностью. Конкретно разделы с 5 по 18 дают соответствующие рекомендации по внедрению и лучшим практикам для поддержки средств управления, указанных в разделах A.5 – A.18 ISO/IEC 27001.

5.4.2 ISO/IEC 27003

Information technology — Security techniques — Guidance

Информационная технология – Методы и средства обеспечения безопасности – Руководство

Область применения: Данный документ содержит пояснения и практические рекомендации по ISO/IEC 27001:2013.

Назначение: ISO/IEC 27003 обеспечивает основу для успешного внедрения СМИБ в соответствии с ISO/IEC 27001.

5.4.3 ISO/IEC 27004

Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

Информационная технология – Методы и средства обеспечения безопасности – Менеджмент информационной безопасности – Мониторинг, измерение, анализ и оценка

Область применения: Данный документ дает рекомендации, предназначенные для помощи организациям в оценке показателей информационной безопасности и результативности СМИБ с целью выполнения требований ISO/IEC 27001. Он рассматривает:

a) мониторинг и измерение показателей информационной безопасности;
b) мониторинг и измерение результативности системы менеджмента информационной безопасности (СМИБ), включая процессы средства управления;
c) анализ и оценку результатов мониторинга и измерений.

Назначение: ISO/IEC 27004 обеспечивает среду, позволяющую измерять и оценивать результативность СМИБ в соответствии ISO/IEC 27001.

5.4.4 ISO/IEC 27005

Information technology — Security techniques — Information security risk management

Информационная технология – Методы и средства обеспечения безопасности – Менеджмент риска информационной безопасности

Область применения: Данный документ содержит рекомендации по менеджменту рисков информационной безопасности. Подход, принятый в данном документе, основывается на общих концепциях, представленных в ISO/IEC 27001.

ISO/IEC 27000:2018

Назначение: ISO/IEC 27005 служит руководством по внедрению процессно-ориентированного подхода к менеджменту риска, чтобы помочь в реализации и выполнении требований к менеджменту рисков информационной безопасности, установленных в ISO/IEC 27001.

5.4.5 ISO/IEC 27007

Information technology — Security techniques — Guidelines for information security management systems auditing

Информационная технология – Методы и средства обеспечения безопасности – Руководящие указания по аудиту систем менеджмента информационной безопасности

Область применения: Данный документ содержит руководство по проведению аудитов СМИБ, а также руководство по обеспечению компетентности аудиторов систем менеджмента информационной безопасности в дополнение к указаниям, содержащимся в ISO 19011, которые применимы к системам менеджмента в целом.

Назначение: ISO/IEC 27007 содержит руководящие указания организациям, которым необходимо проводить внутренние или внешние аудиты СМИБ или управлять программой аудита СМИБ в соответствии с требованиями, установленными в ISO/IEC 27001.

5.4.6 4.4.6 ISO/IEC TR 27008

Information technology — Security techniques — Guidelines for auditors on information security controls

Информационные технологии – Методы обеспечения защиты – Руководящие указания для аудиторов по средствам управления информационной безопасностью

Область применения: Данный документ содержит руководящие указания по проверке внедрения и применения средств управления, включая проверку технического соответствия средств управления информационных систем, согласно установленным в организации стандартам информационной безопасности.

Назначение: Настоящий Технический Отчет делает акцент на проверках соответствия средств управления информационной безопасностью стандарту обеспечения информационной безопасности, который установлен в организации, включая проверки технического соответствия. Он не направлен на обеспечение каких-либо конкретных рекомендаций по проверке соответствия в плане измерений, оценки риска или аудита СМИБ, которые содержатся в ISO/IEC 27004, ISO/IEC 27005 или ISO/IEC 27007 соответственно. Настоящий Технический Отчет не предназначен для аудитов систем менеджмента.

5.4.7 4.4.7 ISO/IEC 27013

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000 -1

Информационная технология – Методы и средства обеспечения безопасности – Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1

Область применения: Данный документ предоставит руководящие указания по интегрированному внедрению стандартов ISO/IEC 27001 и ISO/IEC 20000-1 в организациях, стремящихся к либо:

a) внедрению ISO/IEC 27001 при уже внедренном ISO/IEC 20000-1 или наоборот;

b) совместному внедрению ISO/IEC 27001 и ISO/IEC 20000-1;

c) объединению уже внедренных систем менеджмента в соответствии с ISO/IEC 27001 и ISO/IEC 20000-1.

Назначение: Обеспечить организациям лучшее понимание характеристик, схожести и различий ISO/IEC 27001 и ISO/IEC 20000-1, чтобы помочь при планировании интегрированной системы менеджмента, соответствующей этим двум Международным Стандартам.

5.4.8 4.4.8 ISO/IEC 27014

Information technology — Security techniques — Governance of information security

Информационные технологии – Методы обеспечения безопасности – Руководство по информационной безопасности (*)

Область применения: Данный документ будет содержать принципы и процессы управления информационной безопасностью, посредством которых организация сможет оценивать, направлять и контролировать менеджмент информационной безопасности.

Назначение: Информационная безопасность становится ключевым фактором для организаций. Не только усиление нормативных требований, но также и сбой в функционировании средств обеспечения информационной безопасности в организации может иметь прямое влияние на репутацию организации. Таким образом, от управляющих органов в рамках их общей ответственности все больше требуется уделять внимание информационной безопасности, чтобы гарантировать достижение целей организации.

5.4.9 4.4.9 ISO/IEC TR 27016

Information technology — Security techniques — Information security management – Organizational economics

Информационные технологии – Методы обеспечения безопасности – Менеджмент информационной безопасности – Организационная экономика (*)

Область применения: Настоящий Технический Отчет будет содержать методологию, позволяющую организациям лучшим образом понимать с экономической точки зрения, каким образом более точно определить ценность выявленных информационных активов, оценить потенциальные риски для этих информационных активов, оценить вклад, который вносят средства защиты в ценность этих информационных активов, а также определить оптимальный уровень ресурсов, который необходимо задействовать при защите этих информационных активов.

Назначение: Настоящий Технический Отчет будет дополнять семейство стандартов СМИБ, добавляя экономический аспект в защите информационных активов организации в контексте более широкой социальной среды, в которой действует организация, и предоставит рекомендации, как учитывать экономические аспекты информационной безопасности, на основе моделей и примеров.

5.5 4.5 Стандарты, содержащие рекомендации для специальных областей

5.5.1 4.5.1 ISO/IEC 27010

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

Информационные технологии – Методы обеспечения безопасности – Менеджмент информационной безопасности при обмене информацией между сообществами и организациями (*)

Область применения: Данный документ обеспечивает руководящими указаниями в дополнение к рекомендациям, данным в семействе стандартов ISO/IEC 27000, по

внедрению менеджмента информационной безопасности в сообществах обмена информацией и также определяет средства управления и рекомендации, конкретно связанные с инициированием, поддержанием, обеспечением и улучшением информационной безопасности в обмене информацией между организациями и между сообществами.

Назначение: Данный документ применим ко всем формам обмена и предоставления общего доступа к конфиденциальной информации, как публичной, так и частной, национальной и межнациональной, в рамках одной отрасли или сегмента рынка или между разными. В частности, он может быть применим к обмену, связанному с обеспечением, поддержкой и защитой критически важной инфраструктуры на уровне организации или государства.

5.5.2 4.5.2 ISO/IEC 27011

Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Информационная технология – Методы и средства обеспечения безопасности – Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ISO/IEC 27002

Область применения: Данный документ дает рекомендации, обеспечивающие внедрение менеджмента информационной безопасности в телекоммуникационных компаниях.

Назначение: ISO/IEC 27011 позволяет телекоммуникационным организациям удовлетворять базовые требования по менеджменту информационной безопасности в отношении конфиденциальности, целостности, возможности применения и иных важных аспектов безопасности.

5.5.3 4.5.3 ISO/IEC TR 27015

Information technology — Security techniques - Information security management guidelines for financial services

Информационные технологии – Методы и средства обеспечения безопасности – Рекомендации по менеджменту информации безопасности для финансовых операций

Область применения: Настоящий Технический Отчет обеспечивает руководящими указаниями в дополнение к рекомендациям, данным в семействе стандартов ISO/IEC 27000, по инициированию, внедрению, обеспечению и улучшению информационной безопасности в организациях, оказывающих финансовые услуги.

Назначение: Настоящий Технический Отчет представляет собой специализированное дополнение к Международным Стандартам ISO/IEC 27001 и ISO/IEC 27002 для применения организациями, оказывающими финансовые услуги, чтобы обеспечить их рекомендациями по:

a) инициированию, внедрению, обеспечению и улучшению системы менеджмента информационной безопасности, основанной на требованиях Международного Стандарта ISO/IEC 27001;
b) разработке и внедрению средств управления, определенных в Международном Стандарте ISO/IEC 27002 или в настоящем Международном Стандарте.

5.5.4 4.5.4 ISO/IEC 27017

Information technology — Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Информационные технологии – Методы и средства обеспечения безопасности –

ISO/IEC 27000:2018

Практическое руководство по средствам управления информационной безопасностью, основанных на ISO/IEC 27002, для облачных сервисов

Область применения: ISO/IEC 27017 дает руководящие указания по средствам управления информационной безопасностью, применимым при оказании и использовании облачных услуг, обеспечивая:

— дополнительные рекомендации по внедрению соответствующих средств управления, указанных в ISO/IEC 27002;

— дополнительные средства управления с рекомендациями по внедрению, которые связаны конкретно с облачными сервисами.

Назначение: Данный документ устанавливает средства управления и дает рекомендации по внедрению как для поставщиков, так и пользователей облачных сервисов.

5.5.5 4.5.5 ISO/IEC 27018

Information technology — Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Информационные технологии – Методы и средства обеспечения безопасности – Практическое руководство по защите персональных данных в общедоступных облачных средах, действующих как обработчики персональных данных

Область применения: ISO/IEC 27018 устанавливает общепринятые задачи управления, средства управления и руководящие указания для реализации мер по защите персональных данных (ПД) в соответствии с принципами конфиденциальности, изложенными в ISO/IEC 29100 для общедоступной облачной среды.

Назначение: Данный документ применяется к организациям, включая государственные и частные компании, государственные учреждения и некоммерческие организации, которые предоставляют услуги по обработке информации в качестве обработчиков ПД посредством облачных сервисов по контракту другим организациям. Руководящие указания данного Международного Стандарта могут также оказаться полезными для организаций, выступающих в качестве операторов персональных данных; однако, для операторов персональных данных могут быть дополнительные законодательные и нормативные акты и обязательства по защите персональных данных, не применимые к обработчикам ПД, и они не учитываются в данном Международном Стандарте.

5.5.6 4.5.6 ISO/IEC TR 27019

Information technology — Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

Информационные технологии – Методы и средства обеспечения безопасности – Практическое руководство по средствам управления информационной безопасностью, основанных на ISO/IEC 27002, для облачных сервисов

Область применения: ISO/IEC TR 27019 содержит рекомендации по средствам управления информационной безопасностью, которые должны быть реализованы в системах управления технологическими процессами, используемыми в энергоснабжении для контроля и мониторинга производства, передачи, запасания и распределения электроэнергии, газа и тепла в сочетании с управлением вспомогательными процессами. Это включает, в частности, следующие системы, приложения и компоненты:

— общая IT-поддержка централизованного и распределенного контроля процессов, технологий мониторинга и автоматизации, а также информационных систем, используемых для их функционирования, таких как программаторы и параметризаторы;

— цифровые контроллеры и устройства автоматики, такие как управляющие и периферийные устройства или программируемые логические контроллеры (ПЛК),

включая цифровые датчики и приводные элементы;

— всю дальнейшую поддержку ИТ-систем, используемых в домене управления технологическим процессом, например, для задач визуализации дополнительных данных, а также для целей контроля, мониторинга, архивации данных и документирования;

— общая технология обмена данными, используемая в домене управления технологическими процессами, например, сети, телеметрия, телекоммуникационные приложения и технологии дистанционного управления;

— цифровые приборы учета и средства измерения, например, для измерения объема потребления энергии, выработки или выбросов;

— цифровые системы защиты и обеспечения безопасности, например, реле или ПЛК защиты;

— распределенные компоненты будущих интеллектуальных сетей;

— любое программное обеспечение, прошивки и приложения, установленные на вышеупомянутых системах.

Назначение: В дополнение к целям и мерам по обеспечению безопасности, изложенным в стандарте ISO/IEC 27002, настоящий Технический Отчет содержит рекомендации по средствам управления информационной безопасностью, которые учитывают дополнительные специальные требования, для систем, используемых энергоснабжающими предприятиями и поставщиками энергии.

5.5.7 4.5.4 ISO 27799

Health informatics — Information security management in health using ISO/IEC 27002

Информатизация здоровья — Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002

Область применения: Данный документ содержит рекомендации, обеспечивающие внедрение менеджмента информационной безопасности в организациях здравоохранения.

Назначение: ISO 27779 обеспечивает организации здравоохранения адаптированными под данную отрасль рекомендациями по применению ISO/IEC 27002, которые дополняют рекомендации по выполнению требований Приложения A ISO/IEC 27001.

6 Приложение A

(информационное)

Глагольные формы для формулирования положений

Ни один из стандартов семейства СМИБ не налагает на кого-либо обязательства следовать ему. Однако, такого рода обязательство может возникнуть, например, в законодательном порядке или в силу условий контракта. Для того, чтобы иметь возможность декларировать соответствие с документом, пользователь должен иметь возможность определить требования, которые необходимо выполнить. Пользователь также должен иметь возможность отличать эти требования от рекомендаций, которые дают определенную свободу выбора.

Нижеприведенная таблица дает пояснения, каким образом должны интерпретироваться стандарты семейства СМИБ в части глагольных формулировок, которые либо устанавливают требования, либо служат рекомендациями.

Эта таблица основывается на положениях Части 2:2011 Директив ISO/IEC *Правила для формирования структуры и разработки Международных Стандартов*, Приложение H.

Значение	Пояснение
Требование (requirement)	слова «должен» («shall») и «не должен» («shall not») означают требования, которым необходимо строго следовать для того, чтобы соответствовать документу и никакие отклонения не допустимы
Рекомендация (recommendation)	Слова «следует» («should») или «не следует» («should not») указывают, что среди нескольких возможностей одна рекомендуется как наиболее подходящая без упоминания или исключения других, или что определенное направление действий является более предпочтительным, но не обязательным, или что (в отрицательной форме) определенная возможность или направление действий не рекомендованы, хотя и не запрещены
Разрешение (permission)	Слово «может» («may») или «не требуется» («need not») указывает направление действий, допустимое в рамках документа
Возможность (possibility)	Слово «может» («can») или «не может» («cannot») указывает на возможность чего-либо

7 Приложение B

(информативное)

Термины и ответственность за терминологию

B.1 Ответственность за терминологию

Устанавливающий терминологию для семейства стандартов ISO/IEC 27000 – **стандарт**, который первоначально определяет термины. Устанавливающий терминологию также отвечает за поддержку актуальности определений, т.е.

- предоставление,
- пересмотр,
- обновление, и
- исключение.

Примечание 1 ISO/IEC 27000 сам никогда не определяется как устанавливающий терминологию.

Примечание 2 ISO/IEC 27001 и ISO/IEC 27006 в качестве нормативных стандартов (т.е. содержащих требования) всегда имеют приоритет, как соответствующие устанавливающие терминологию

B.1 Термины, использованные в вышеуказанных Международных Стандартах

B.2.1 ISO/IEC 27001

аудит (audit)	2.5	измерение (measurement)	2.48
возможность применения (availability)	2.9	мониторинг (monitoring)	2.52
компетентность (competence)	2.11	несоответствие (non-conformity)	2.53
конфиденциальность (confidentiality)	2.12	цель (objective)	2.56
соответствие (conformity)	2.13	организация (organization)	2.57
постоянное улучшение (continual improvement)	2.15	передавать на аутсорсинг (outsource)	2.58
средство управления (control)	2.16	показатель деятельности (performance)	2.59
коррекция (correction)	2.18	политика (policy)	2.60
корректирующее действие (corrective action)	2.19	процесс (process)	2.61
документированная информация (documented information)	2.23	требование (requirement)	2.63
результативность (effectiveness)	2.24	анализ (review)	2.65
информационная безопасность (information security)	2.33	риск (risk)	2.68
целостность (integrity)	2.40	владелец риска (risk owner)	2.78
заинтересованные стороны (interested party)	2.41	высшее руководство (top management)	2.84
система менеджмента (management	2.46		

system)

B.2.2 ISO/IEC 27002

контроль доступа (access control)	2.1	событие информационной безопасности (information security event)	2.35
атака (attack)	2.3	инцидент информационной безопасности (information security incident)	2.36
аутентификация (authentication)	2.7	менеджмент инцидентов информационной безопасности (information security incident management)	2.37
подлинность (authenticity)	2.8	информационная система (information system)	2.39
задача управления (control objective)	2.17	неопровержимость авторства (non-repudiation)	2.54
устройства обработки информации (information processing facilities)	2.32	надежность (reliability)	2.62
непрерывность информационной безопасности (information security continuity)	2.34		

B.2.3 ISO/IEC 27003

проект СМИБ (ISMS project)	2.43

B.2.4 ISO/IEC 27004

аналитическая модель (analytical model)	2.2	функция измерения (measurement function)	2.49
атрибут (attribute)	2.4	метод измерения (measurement method)	2.50
основной показатель (base measure)	2.10	результаты измерения (measurement results)	2.51
данные (data)	2.20	объект (object)	2.55
критерий принятия решения (decision criteria)	2.21	шкала (scale)	2.80
производный показатель (derived measure)	2.22	единица измерения (unit of measurement)	2.86
параметр (indicator)	2.30	валидация (validation)	2.87
потребность в информации (informational need)	2.31	верификация (verification)	2.88
показатель (measure)	2.47		

B.2.5 ISO/IEC 27005

последствие (consequence)	2.14	обмен информацией по рискам и консультации (risk communication and consultation)	2.72
событие (event)	2.25	критерий риска (risk criteria)	2.73
внешний контекст (external context)	2.27	определение степени риска (risk evaluation)	2.74
внутренний контекст (internal context)	2.42	идентификация риска (risk identification)	2.75
уровень риска (level of risk)	2.44	менеджмент риска (risk management)	2.76
вероятность (likelihood)	2.45	процесс менеджмента риска (risk management process)	2.77
остаточный риск (residual risk)	2.64	обработка риска (risk treatment)	2.79
принятие риска (risk acceptance)	2.69	угроза (threat)	2.83
анализ риска (risk analysis)	2.70	уязвимость (vulnerability)	2.89
оценка риска (risk assessment)	2.71		

B.2.6 ISO/IEC 27006

документ сертификации (certification body)

маркировка (mark)

B.2.7 ISO/IEC 27007

область аудита (audit scope) 2.6

B.2.8 ISO/IEC 27008

объект анализа (review object)	2.66	стандарт обеспечения безопасности (security implementation standard)	2.81
цель анализа (review objective)	2.67		

B.2.9 ISO/IEC 27010

сообщество обмена информацией (information sharing community)	2.38	доверенный участник информационного сообщества (trusted information communication entity)	2.85

B.2.10 ISO/IEC 27011

совместное размещение (collocation)	телекоммуникационные средства (telecommunications facilities)
узел связи (communication centre)	телекоммуникационные организации (telecommunications organizations)
важнейшие коммуникации (essential	телекоммуникационные записи

communication)

неразглашение [информации о] соединениях (non-disclosure of communications)

персональная информация (personal information)

приоритетный вызов (priority call)

телекоммуникационные прикладные программы (telecommunications applications)

телекоммуникационный бизнес (telecommunications business)

телекоммуникационная аппаратная (telecommunications equipment room)

(telecommunications records)

телекоммуникационные услуги (telecommunications services)

клиент телекоммуникационных услуг (telecommunications services customer)

пользователь телекоммуникационных услуг (telecommunications services user)

терминальное оборудование (terminal facilities)

пользователь (user)

B.2.11 ISO/IEC 27014

высшее исполнительное руководство (executive management)	2.26	руководящий орган управления (governing body)	2.29
управление информационной безопасностью (governance of information security)	2.28	влияющая сторона (stakeholder)	2.82

B.2.12 ISO/IEC TR 27015

финансовые услуги (financial services)

B.2.13 ISO/IEC TR 27016

ожидаемые годовые потери (annualized loss expectancy, ALE)

потери (loss)

прямая стоимость (direct value)

рыночная стоимость (market value)

экономическое сопоставление (economic comparison)

чистая приведенная стоимость (net present value)

экономический фактор (economic factor)

внеэкономическая выгода (non economic benefit)

экономическое обоснование (economic justification)

приведенная стоимость (present value)

экономическая добавленная стоимость (economic added value)

альтернативные издержки (opportunity cost)

экономика (economics)

альтернативная стоимость (opportunity value)

оценочная стоимость (expected value)

нормативные требования (regulatory requirements)

продленная ценность (extended value)

коэффициент рентабельности инвестиций (return on investment)

косвенная стоимость (indirect value)

общественная ценность (societal value)

ISO/IEC 27000:2018

экономика информационной безопасности (information security economics)

менеджмент информационной безопасности (information security management IMS)

стоимость (value)

стоимостная мера риска (value-at-risk)

B.2.14 ISO/IEC TR 27017

способность (capability)

утечка данных (data breach)

архитектура коллективного пользования с гарантированным обеспечением безопасности (secure multi-tenancy)

виртуальная машина (virtual machine)

B.2.15 ISO/IEC TR 27018

утечка данных (data breach)

персональные данные, ПД (personally identifiable information, PII)

оператор ПД (PII controller)

обладатель ПД (PII principal)

обработчик персональных данных (PII processor)

обработка персональных данных (processing of PII)

поставщик общедоступных облачных сервисов (public cloud service provider)

B.2.16 ISO/IEC TR 27019

прекращение подачи электроэнергии (blackout)

группа реагирования на компьютерные инциденты (Computer Emergency Response Team, CERT)

ключевая инфраструктура (critical infrastructure)

отладка (debugging)

энергоснабжение (energy supply)

энергоснабжающая организация (energy utility)

интерфейс человек-машина (human-machine interface, HMI)

обслуживание (maintenance)

программируемый логический контроллер, ПЛК (PLC)

система контроля технологических процессов(process control system)

безопасность (safety)

заявление о применимости (statement of applicability, SOA)

система передачи (transmission system)

8 Библиография

[1] ISO/IEC 17021, *Conformity assessment — Requirements for bodies providing audit and certification of management systems*
[2] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*
[3] ISO 19011:2011, *Guidelines for auditing management systems*
[4] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
[5] ISO/IEC 27002, *Information technology — Security Techniques — Code of practice for information security controls*
[6] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*
[7] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*
[8] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
[9] ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*
[10] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*
[11] ISO/IEC TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*
[12] ISO/IEC 27009, *Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements*
[13] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*
[14] ISO/IEC 27011, *Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*
[15] ISO/IEC 27013, *Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1*
[16] ISO/IEC 27014, *Information technology — Security techniques — Governance of information security*
[17] ISO/IEC TR 27015, *Information technology — Security techniques — Information security management guidelines for financial services*
[18] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
[19] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
[20] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
[21] ISO/IEC 27019, *Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*
[22] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
[23] ISO Guide 73:2009, *Risk management — Vocabulary*
[24] ISO/IEC 15939:2007, *Systems and software engineering — Measurement process*
[25] ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*