ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27000— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Системы менеджмента информационной безопасности. Общий обзор и терминология

(ISO/IEC 27000:2018, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Акционерным обществом «Эксперт» (АО «Эксперт») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 392-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27000:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (ISO/IEC 27000:2018 «Information technology — Security techniques — Information security management systems — Overview and vocabulary», IDT).

ИСО/МЭК 27000 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 27000—2012

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. ИСО и МЭК не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

0.1 Общие сведения

Международные стандарты системы менеджмента предоставляют модель для применения при создании и функционировании системы менеджмента. Данная модель предусматривает элементы, на основе которых эксперты данной области достигли согласия с учетом лучшей международной практики. В состав подкомитета ПК 27 Совместного технического комитета ИСО/МЭК СТК 1 входит комиссия экспертов, занимающаяся разработкой семейства международных стандартов по информационной безопасности (ИБ), известного как семейство стандартов системы менеджмента информационной безопасности (СМИБ).

Используя семейство стандартов СМИБ, организации могут разрабатывать и совершенствовать систему управления защитой информационных активов и подготовиться к независимой оценке своей СМИБ, применяемой для защиты различного рода информации, например, финансовых данных, интеллектуальной собственности, сведений о персонале, а также информации, доверенной клиентами или третьей стороной.

0.2 Цель настоящего стандарта[1)]

В состав семейства стандартов СМИБ входят стандарты, которые:

a) определяют требования к СМИБ и к органам, сертифицирующим такие системы;

b) обеспечивают непосредственную поддержку, содержат подробные рекомендации и/или интерпретацию общего процесса разработки, внедрения, поддержки и совершенствования СМИБ;

c) содержат руководства по СМИБ для конкретных отраслей;

d) содержат указания по оценке соответствия СМИБ.

0.3 Общие указания настоящего стандарта

В настоящем стандарте используются следующие формулировки:

- «должен» означает обязательное требование;
- «следует» означает рекомендацию;
- «вправе» означает разрешение;
- «может» означает возможность или способность.

Информация, обозначенная как «П р и м е ч а н и е », уточняет или разъясняет содержание требования. В примечаниях в разделе 3 содержится информация, которая дополняет определение терминов, также могут встречаться положения, регулирующие использование того или иного термина.

[1)] *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных актов и стандартов Российской Федерации в области защиты информации.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Системы менеджмента информационной безопасности. Общий обзор и терминология

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

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит общий обзор систем менеджмента информационной безопасности (СМИБ). В нем приведены термины и определения, используемые в семействе стандартов СМИБ. Настоящий стандарт применим к организациям любого типа и размера (например, коммерческим предприятиям, правительственным учреждениям, некоммерческим организациям).

Термины и определения, представленные в настоящем стандарте:

- охватывают общие термины и определения, используемые в семействе стандартов СМИБ;
- не охватывают все термины и определения, применяемые в семействе стандартов СМИБ;
- не ограничивают применение новых терминов в семействе стандартов СМИБ.

2 Нормативные ссылки

В настоящем стандарте отсутствуют нормативные ссылки.

3 Термины и определения

ИСО и МЭК поддерживают терминологические базы, используемые в сфере стандартизации, доступные на следующих сайтах:

- Онлайн-библиотека стандартов ISO: https://www.iso.org/obp;
- IEC Electropedia: https://www.electropedia.org/

3.1 **управление доступом** (access control): Обеспечение санкционированного доступа к активам в соответствии с бизнес-требованиями и требованиями (3.56) безопасности.

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

3.3 **аудит** (audit): Систематический, независимый и задокументированный процесс (3.54), предназначенный для получения свидетельств аудита и объективной оценки аудиторами степени соблюдения критериев аудита.

Примечания

1 Аудит может быть внутренним (первой стороны), внешним (второй или третьей стороны) или комбинированным (сочетание двух и более сторон).

2 Внутренний аудит проводится самой организацией или сторонней (внешней) организацией.

3 Термины «свидетельства аудита» и «критерии аудита» определены в ИСО 19011.

Издание официальное

3.4 **область аудита** (audit scope): Объем и границы аудита (3.3).

[ИСО 19011:2011, статья 3.14, с изменениями — примечание 1 было удалено]

3.5 **аутентификация** (authentication): Обеспечение гарантии того, что заявленные характеристики субъекта и объекта являются подлинными[1)].

3.6 **подлинность** (authenticity): Свойство, определяющее, что фактический субъект или объект совпадает с заявленным.

3.7 **доступность** (availability): Свойство, определяющее возможность использования объекта авторизованным субъектом по запросу.

3.8 **основной показатель** (base measure): Показатель (3.42), определенный в терминах атрибута и метода для его количественного определения.

Примечание — Основной показатель функционально не зависит от других показателей.

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.3, с изменениями — примечание 2 было удалено]

3.9 **компетентность** (competence): Способность применять знания и навыки для достижения намеченных результатов.

3.10 **конфиденциальность** (confidentiality): Недоступность для неавторизованных лиц, объектов или процессов (3.54).

3.11 **соответствие** (conformity): Выполнение требования (3.56).

3.12 **последствие** (consequence): Результат события (3.21), оказывающего влияние на достижение цели (3.49).

Примечания

1 Результатом воздействия события может быть целый ряд последствий.

2 Последствия могут быть определенными или неопределенными и в контексте информационной безопасности, как правило, носят негативный характер.

3 Последствия могут оцениваться качественно или количественно.

4 Первоначальные последствия могут усугубляться из-за эффекта цепной реакции.

[Руководство ИСО 73:2009, статья 3.6.1.3, с изменениями — примечание 2 было изменено после «и»]

3.13 **постоянное улучшение** (continual improvement): Действия по повышению производительности (3.52), осуществляемые по регламенту с определенной периодичностью.

3.14 **мера обеспечения информационной безопасности** (control): Мера, направленная на изменение риска (3.61).

Примечания

1 К мерам обеспечения информационной безопасности относятся процессы (3.54), политика (3.53), устройства, практические приемы или другие действия, используемые для изменения риска (3.61).

2 Меры обеспечения информационной безопасности не всегда могут приводить к запланированным или предполагаемым изменениям риска.

[Руководство ИСО 73:2009, статья 3.8.1.1, с изменениями примечания 2]

3.15 **цель применения мер** (control objective): Описание того, что должно быть достигнуто в результате применения мер обеспечения информационной безопасности (3.14).

3.16 **коррекция** (correction): Действие по устранению выявленного несоответствия (3.47).

3.17 **корректирующее действие** (corrective action): Действие, позволяющее устранить причину несоответствия (3.47) и предотвратить его повторение в будущем.

3.18 **производный показатель** (derived measure): Показатель (3.42), определяемый как функция от двух или более значений основных показателей (3.8).

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.8, с изменениями — примечание 1 было удалено]

3.19 **документированная информация** (documented information): Информация, которая должна управляться и поддерживаться организацией (3.50), и носитель, который ее содержит.

Примечания

1 Документированная информация может иметь любой формат, быть записана на любом типе носителя и поступать из любого источника.

[1)] *Данное определение по смыслу соответствует определению по ГОСТ Р 58833—2020 «Защита информации. Идентификация и аутентификация. Общие положения».*

2 Документированная информация может относиться:
- к системе менеджмента (3.41), включая связанные с ней процессы (3.54);
- к информации, создаваемой для функционирования организации (3.50) (документация);
- к доказательствам достигнутых результатов (записям).

3.20 **эффективность** (effectiveness): Степень реализации запланированных мероприятий и достижения намеченных результатов.

3.21 **событие** (event): Возникновение или изменение определенного набора условий.

Примечания

1 Событие может быть единичным или многократным и иметь несколько причин.

2 Событие может быть определенным или неопределенным.

3 Событие может иногда называться «инцидентом» или «происшествием».

[Руководство ИСО 73:2009, статья 3.5.1.3, с изменениями — примечание 4 было удалено]

3.22 **внешний контекст** (external context): Внешняя среда, в которой организация стремится к достижению своих целей (3.49).

Примечание — Внешняя среда может включать в себя следующее:
- внешнюю среду, связанную с культурной, социальной, политической, законодательной, регулирующей, экономической, природной или конкурентной сферой на международном, национальном, региональном или местном уровне;
- ключевые критерии и тенденции, которые могут воздействовать на достижение установленных целей организации (3.50);
- взаимоотношения с внешними заинтересованными сторонами, восприятие ими риска и значимость для организации этих заинтересованных сторон (3.37).

[Руководство ИСО 73:2009, статья 3.3.1.1]

3.23 **руководство деятельностью по обеспечению информационной безопасности** (governance of information security): Система, с помощью которой контролируется и управляется деятельность организации (3.50) в области обеспечения информационной безопасности (3.28).

3.24 **руководящий орган** (governing body): Лицо или группа лиц, несущих ответственность за производительность (3.52) организации (3.50) и за соблюдение ею применяемых норм.

Примечание — В некоторых юрисдикциях руководящим органом может быть совет директоров.

3.25 **индикатор** (indicator): Показатель (3.42), используемый для расчета или оценки.

3.26 **информационная потребность** (information need): Знание, необходимое для управления задачами, целями (3.49), рисками и проблемами.

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.12]

3.27 **средства обработки информации** (information processing facilities): Совокупность автономных устройств сбора, накопления, передачи, обработки и представления информации.

3.28 **информационная безопасность (ИБ)** (information security): Сохранение конфиденциальности (3.10), целостности (3.36) и доступности (3.7) информации.

Примечание — Этот термин может включать в себя и другие дополнительные свойства, такие как подлинность (3.6), подотчетность, неотказуемость (3.48) и достоверность (3.55).

3.29 **обеспечение непрерывности информационной безопасности** (information security continuity): Процессы (3.54) и процедуры, гарантирующие непрерывность операций по обеспечению информационной безопасности (3.28).

3.30 **событие информационной безопасности** (information security event): Выявленное состояние системы, услуги или сети, указывающее на возможное нарушение политики (3.53) обеспечения информационной безопасности (3.28) или сбой мер обеспечения информационной безопасности (3.14), или ранее неизвестная ситуация, которая может иметь отношение к вопросам безопасности.

3.31 **инцидент информационной безопасности** (information security incident): Одно или несколько нежелательных или неожиданных событий информационной безопасности (3.30), которые с высокой степенью вероятности могут привести к компрометации в бизнес-процессах и создают угрозы для информационной безопасности (3.28).

3.32 **менеджмент инцидентов информационной безопасности** (information security incident management): Совокупность процессов (3.54) обнаружения, информирования, оценки, реагирования,

рассмотрения инцидентов информационной безопасности (3.31) и извлечения соответствующего полезного опыта.

3.33 **специалист (администратор) системы менеджмента информационной безопасности (СМИБ)** (information security management system (ISMS) professional): Лицо, которое устанавливает, внедряет, поддерживает и постоянно совершенствует один или несколько процессов (3.54) системы менеджмента информационной безопасности.

3.34 **сообщество по обмену информацией** (information sharing community): Группа организаций (3.50), которые согласны обмениваться информацией.

Примечание — В качестве организации может выступать физическое лицо.

3.35 **информационная система** (information system): Набор приложений, услуг, информационно-технических активов или других компонентов для обработки информации.

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

3.37 **заинтересованная сторона** (предпочтительный термин) [interested party (preferred term)]
участник (допустимый термин) [stakeholder (admitted term)]: Лицо или организация (3.50), способные влиять на какое-либо решение или действия.

3.38 **внутренний контекст** (internal context): Внутренняя среда, в которой организация стремится к достижению своих целей.

Примечание — Внутренняя среда может включать в себя:
- управление, организационную структуру, обязанности и подотчетность;
- политику (3.53), цели (3.49) и стратегии, направленные на их достижение;
- возможности организации с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы (3.54), системы и технологии);
- информационные системы (3.35), информационные потоки и процессы принятия решений (формальные и неформальные);
- взаимоотношения с внутренними заинтересованными сторонами, восприятие ими риска и значимость для организации этих заинтересованных сторон (3.37);
- культуру организации;
- стандарты, руководящие принципы и модели работы, принятые организацией;
- форму и объем договорных отношений.

[Руководство ИСО 73:2009, статья 3.3.1.2]

3.39 **уровень риска** (level of risk): Мера риска (3.61), выраженная в виде сочетания последствий (3.12) и их вероятности (3.40).

[Руководство ИСО 73:2009, статья 3.6.1.8, с изменениями — фраза «или комбинация рисков» исключена из определения]

3.40 **вероятность** (likelihood): Степень возможности наступления какого-либо события.

[Руководство ИСО 73:2009, статья 3.6.1.1, с изменениями — примечания 1 и 2 были удалены]

3.41 **система менеджмента** (management system): Набор политик (3.53), целей (3.49) и процессов (3.54), используемых организацией (3.50) для достижения этих целей.

Примечания

1 Система менеджмента может охватывать один или несколько аспектов.

2 К элементам такой системы относятся организационная структура, роли и обязанности, процессы планирования и функционирования.

3 Сфера действия системы менеджмента может охватывать организацию в целом, конкретные выявленные функции или сегменты организации, а также одну (несколько) функций в рамках группы организаций.

3.42 **показатель** (measure): Переменная, которой присваивается какое-либо значение как конкретный результат измерения (3.43).

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.15, с изменениями — примечание 2 было удалено]

3.43 **измерения** (measurement): Процесс (3.54) определения значения.

3.44 **функция измерения** (measurement function): Алгоритм или расчет, выполненный для комбинации двух или более основных показателей (3.8).

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.20]

3.45 **метод измерения** (measurement method): Логическая последовательность описанных в общих чертах операций, используемая для количественной оценки атрибута относительно заданной шкалы.

Примечание — Тип метода измерения зависит от природы операций, используемых для количественной оценки атрибута. Можно выделить два типа:

- субъективный: количественная оценка на основе человеческого суждения;
- объективный: количественная оценка на основе численных методов.

[ИСО/МЭК/ИИЭР 15939:2017, статья 3.21, с изменениями — примечание 2 было удалено]

3.46 **мониторинг** (monitoring): Определение состояния системы, процесса (3.54) или вида деятельности.

Примечание — Для определения состояния может потребоваться проверка, наблюдение или критическое наблюдение.

3.47 **несоответствие** (nonconformity): Несоблюдение требования (3.56).

3.48 **неотказуемость** (non-repudiation): Способность удостоверять имевшее место событие (3.21) или действие, которые в дальнейшем не могут быть поставлены под сомнение.

3.49 **цель** (objective): Ожидаемый результат.

Примечания

1 Цель может быть стратегической, тактической или операционной.

2 Цели могут относиться к различным аспектам (например, существуют финансовые, медицинские, экологические цели и цели обеспечения безопасности) и применяться на различных уровнях [стратегическом, организационном, проектном, продуктовом и процессном (3.54)].

3 Цель может быть выражена другим способом, например, как предполагаемый результат, намерение, операционный критерий, задача информационной безопасности или путем использования других слов с аналогичным значением (например, стремление, намерение, плановый показатель).

4 В контексте систем менеджмента информационной безопасности цели информационной безопасности устанавливаются организацией согласно политике информационной безопасности для достижения конкретных результатов.

3.50 **организация** (organization): Лицо или группа лиц, наделенных определенными функциями, областями ответственности, полномочиями и взаимоотношениями для достижения своих целей (3.49).

Примечание — Под «организацией» понимают, помимо прочего, индивидуальных предпринимателей, компании, корпорации, фирмы, партнерства, благотворительные организации, учреждения, любые составные части и сочетания названных объектов вне зависимости от того, зарегистрирована ли организация в качестве юридического лица, является ли она государственной или частной.

3.51 **аутсорсинг** (outsource): Договоренность о том, что внешняя организация (3.50) выполняет часть функции или процесса (3.54) организации.

Примечание — Внешняя организация находится вне сферы охвата системы менеджмента (3.41), однако функция или процесс, переданные на внешний подряд, входят в эту сферу.

3.52 **производительность** (performance): Результат измерений.

Примечания

1 Показатели производительности могут иметь отношение как к количественным, так и к качественным выводам.

2 Производительность может относиться к управлению деятельностью, процессами (3.54), продуктами (включая услуги), системами или организациями (3.50).

3.53 **политика** (policy): Намерения и направления деятельности организации (3.50), официально выраженные ее высшим руководством (3.75).

3.54 **процесс** (process): Набор взаимосвязанных или взаимодействующих мероприятий, в результате которых исходные ресурсы преобразуются в конечный продукт.

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

3.56 **требование** (requirement): Заявленная потребность или ожидание, обычно подразумеваемые или обязательные.

Примечания

1 «Обычно подразумеваемые» означает, что заявленная потребность или ожидание рассматриваются в соответствии со стандартной или общепринятой практикой организации и заинтересованных сторон.

2 Указанным требованием является требование, изложенное, например, в документированной информации.

3.57 **остаточный риск** (residual risk): Риск (3.61), остающийся после обработки риска (3.72).

Примечания

1 Остаточный риск может содержать неопределенный риск.

2 Остаточный риск может также называться «сохраненным риском».

3.58 **проверка** (review): Деятельность, предпринимаемая для анализа пригодности, адекватности, эффективности (3.20) рассматриваемого объекта по отношению к достижению установленных целей (3.49).

[Руководство ИСО 73:2009, статья 3.8.2.2, с изменениями — примечание 1 было удалено]

3.59 **объект проверки** (review object): Конкретный проверяемый объект.

3.60 **цель проверки** (review objective): Формулировка, характеризующая, чего следует достичь в результате проверки (3.58).

3.61 **риск** (risk): Влияние неопределенности на достижение целей (3.49).

Примечания

1 Следствием влияния является отклонение (как в положительную сторону, так и в отрицательную) от ожидаемого результата.

2 Неопределенность представляет собой состояние, в том числе частичное, отсутствия информации о событии, его последствиях или вероятности его наступления.

3 Зачастую риск описывается как потенциальное событие (в соответствии с определением, приведенном в Руководстве ИСО 73:2009, статья 3.5.1.3) и его последствия (в соответствии с определением, приведенным в Руководстве ИСО 73:2009, статья 3.6.1.3) или как их сочетание.

4 Риск обычно описывается сочетанием последствий события (в том числе изменений обстоятельств) и вероятности (в соответствии с определением, приведенном в Руководстве ИСО 73:2009, статья 3.6.1.1) их возникновения.

5 В контексте систем менеджмента информационной безопасности риски в области информационной безопасности могут выражаться в виде влияния неопределенности на цели информационной безопасности.

6 Риск в области информационной безопасности связан с возможностью того, что угрозы будут эксплуатировать уязвимости того или иного информационного актива (группы таких активов) и тем самым причинят вред организации.

3.62 **принятие риска** (risk acceptance): Обоснованное решение о принятии риска (3.61).

Примечания

1 Решение о принятии риска может быть принято без обработки риска (3.72) или в процессе (3.54) обработки риска.

2 Необходимо проводить мониторинг (3.46) и проверки (3.58) принятого риска.

[Руководство ИСО 73:2009, статья 3.7.1.6]

3.63 **анализ риска** (risk analysis): Процесс (3.54) изучения природы и характера риска (3.61) и определения уровня риска (3.39).

Примечания

1 Анализ риска обеспечивает основу для проведения оценивания риска (3.67) и принятия решения об обработке риска (3.72).

2 Анализ риска включает в себя установление значения риска.

[Руководство ИСО 73:2009, статья 3.6.1]

3.64 **оценка риска** (risk assessment): Процесс (3.54), охватывающий идентификацию риска (3.68), анализ риска (3.63) и оценивание риска (3.67).

[Руководство ИСО 73:2009, статья 3.4.1]

3.65 **передача информации о риске и консультация** (risk communication and consultation): Набор непрерывных и повторяющихся процессов (3.54), которые организация осуществляет для предоставления и получения информации либо для обмена ею, а также для участия в диалоге с заинтересованными сторонами (3.37) по вопросам менеджмента риска (3.61).

Примечания

1 Информация может относиться к наличию, природе, форме, вероятности (3.40), значимости, оценке, приемлемости и обработке риска.

2 Консультация представляет собой двусторонний процесс содержательного обмена информацией между организацией (3.50) и ее заинтересованными сторонами по тому или иному вопросу до принятия решения или определения направления деятельности по соответствующему вопросу. Консультация представляет собой:

- процесс, который влияет на принятие решения посредством авторитета, а не посредством власти;
- предварительный этап принятия решения, а не совместное принятие решения.

3.66 **критерии риска** (risk criteria): Совокупность факторов, по сопоставлению с которыми оценивают значимость риска (3.61).

Примечания

1 Критерии риска основаны на установленных целях организации, на внешнем (3.22) и внутреннем контексте (3.38) ее деятельности.

2 Критерии риска могут быть сформированы на основе требований стандартов, политики (3.53), законодательных и других требований (3.56).

[Руководство ИСО 73:2009, статья 3.3.1.3]

3.67 **оценивание 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 приемлемой или допустимой.

Примечание — Оценивание риска может быть использовано при принятии решения об обработке риска (3.72).

[Руководство ИСО 73:2009, статья 3.7.1]

3.68 **идентификация риска** (risk identification): Процесс (3.54) обнаружения, осознания и описания риска (3.61).

Примечания

1 Элементы риска могут включать в себя источники риска, событий (3.21), их причин и возможные последствия (3.12).

2 Идентификация рисков может включать в себя теоретический анализ, анализ хронологических данных, экспертных оценок и потребностей заинтересованных сторон (3.37).

[Руководство ИСО 73:2009, статья 3.5.1]

3.69 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией (3.50) в области риска (3.61).

[Руководство ИСО 73:2009, статья 2.1]

3.70 **процесс менеджмента риска** (risk management process): Систематическое применение политики (3.53), процедур и практических методов в области управления деятельностью по информированию, консультированию, определению контекста и выявлению, анализу, оценке, обработке, мониторингу и проверке рисков (3.61).

Примечание — В ИСО/МЭК 27005 термин «процесс» (3.54) используется для описания управления рисками в целом. Элементы процесса менеджмента риска (3.69) называются «мероприятиями».

[Руководство ИСО 73:2009, статья 3.1, с изменениями — добавлено примечание]

3.71 **владелец риска** (risk owner): Лицо или организация, обладающие ответственностью и полномочиями по менеджменту риска (3.61).

[Руководство ИСО 73:2009, статья 3.5.1.5]

3.72 **обработка риска** (risk treatment): Процесс (3.54) управления риском (3.61).

Примечания

1 Обработка риска может включать в себя:

- исключение риска путем отказа от начала или продолжения деятельности, являющейся источником риска;
- принятие риска или повышение его уровня для обеспечения определенной возможности;
- устранение источников риска;
- изменение вероятности (3.40);
- изменение последствий (3.12);
- разделение риска с другой стороной или сторонами (путем включения в контракты или финансирования обработки риска);
- обоснованное решение о сохранении риска.

2 Обработка рисков, связанная с негативными последствиями, иногда называется снижением, устранением или предотвращением риска.

3 Обработка риска может создавать новые риски или модифицировать существующие.

[Руководство ИСО 73:2009, статья 3.8.1, с изменениями — «решение» было заменено на «выбор» в примечании 1]

3.73 **стандарт реализации безопасности** (security implementation standard): Документ, определяющий разрешенные способы обеспечения безопасности.

3.74 **угроза** (threat): Потенциальная причина нежелательного инцидента, который может нанести вред системе или организации (3.50).

3.75 **высшее руководство** (top management): Лицо или группа лиц, руководящих организацией (3.50) и контролирующих ее на высшем уровне.

Примечания

1 Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы в рамках организации.

2 Если область применения системы менеджмента (3.41) охватывает только часть организации, то высшее руководство относится к тем, кто руководит этой частью организации и контролирует ее.

3 Высшее руководство иногда именуется исполнительным руководством и может включать в себя главных исполнительных директоров, финансовых директоров, директоров по информационным технологиям и аналогичных должностных лиц.

3.76 **доверенная структура передачи информации** (trusted information communication entity): Автономная организация (3.50), поддерживающая обмен информацией в рамках сообщества по обмену информацией (3.34).

3.77 **уязвимость** (vulnerability): Слабое место актива или меры обеспечения информационной безопасности (3.14), которое может быть использовано одной или несколькими угрозами (3.74).

4 Системы менеджмента информационной безопасности (СМИБ)

4.1 Общая информация

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, стоящих перед организацией;

c) сталкиваются с рядом рисков, которые могут оказывать воздействие на функционирование активов организации;

d) принимают меры в отношении предполагаемого воздействия рисков, осуществляя внедрение мер обеспечения ИБ.

Вся информация, хранящаяся и обрабатывающаяся организацией, подвержена угрозам компьютерных атак, ошибкам, стихийным бедствиям (например, наводнению или пожару) и т. д., а также является объектом влияния уязвимостей, присущих ее использованию. Термин «информационная безопасность» относится к информации, которую рассматривают как актив, представляющий собой ценность, требующую соответствующей защиты, например, от потери доступности, конфиденциальности и целостности. Обеспечение возможности санкционированного своевременного получения точной и полной информации способствует эффективности бизнеса.

Защита информационных активов посредством определения, достижения, поддержания и улучшения ИБ имеет важное значение для того, чтобы обеспечить достижение намеченных организацией целей, а также поддерживать и повышать уровень соответствия законодательным нормам и репутацию организации. Эти скоординированные действия, направленные на внедрение соответствующих мер обеспечения информационной безопасности и обработку недопустимых рисков в области ИБ, широко известны как элементы менеджмента ИБ.

Так как риски ИБ и эффективность мер обеспечения ИБ меняются в зависимости от обстоятельств, организациям необходимо:

a) контролировать и оценивать эффективность внедренных мер обеспечения ИБ и процедур;

b) идентифицировать появляющиеся риски для их обработки;

c) выбирать, внедрять и совершенствовать должным образом соответствующие меры обеспечения ИБ.

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

4.2 Что такое СМИБ?

4.2.1 Общие сведения и принципы

Система менеджмента информационной безопасности (СМИБ) включает в себя политику, процедуры, руководящие принципы и связанные с ними ресурсы и мероприятия, коллективно управляемые организацией в целях защиты ее информационных активов. СМИБ обеспечивает системный подход к созданию, внедрению, функционированию, мониторингу, анализу, поддержке и усилению ИБ организации для достижения бизнес-целей. Она основывается на оценке рисков и уровнях принятия рисков организацией, предназначенных для эффективной обработки рисков и управления ими. Анализ требований по защите информационных активов и применение соответствующих мер, обеспечивающих необходимую защиту этих активов, способствуют успешному внедрению СМИБ. Для успешного внедрения СМИБ организации должны соблюдать следующие основные принципы:

a) понимание необходимости использования СМИБ;

b) назначение ответственности за обеспечение ИБ;

c) обеспечение баланса между обязательствами руководства и потребностями заинтересованных сторон;

d) повышение социальной значимости;

e) оценивание рисков, чтобы применять необходимые меры обеспечения ИБ для достижения допустимых уровней рисков;

f) обеспечение безопасности неотъемлемых элементов информационных сетей и систем;

g) активное предупреждение и выявление инцидентов ИБ;

h) применение комплексного подхода к менеджменту ИБ;

i) регулярное переоценивание уровня ИБ и внесение соответствующих изменений.

4.2.2 Информация

Информация — это актив, который наряду с другими важными активами представляет собой огромную ценность для бизнеса организации и, следовательно, должен быть надежно защищен. Информация может существовать в различной форме, в том числе в цифровом формате (например, в виде файлов с данными, записанных на электронных или оптических носителях), в материальном виде (например, быть записанной или напечатанной на бумаге), а также в нематериальном виде — знания сотрудников. Информация может передаваться различными способами: с помощью курьера, систем электронной почты или голосовой связи. Независимо от формы и способа передачи информации она должна быть надежно защищена.

Во многих организациях существует зависимость между информацией и информационно-коммуникационными технологиями (ИКТ). ИКТ-технологии являются важнейшим элементом любой организации. Они облегчают создание, обработку, хранение, передачу, защиту и уничтожение информации.

4.2.3 Информационная безопасность

ИБ обеспечивает конфиденциальность, доступность и целостность информации. Чтобы гарантировать успешное ведение бизнеса в долгосрочной перспективе и свести к минимуму негативное воздействие, ИБ предусматривает применение и администрирование соответствующих мер обеспечения ИБ, учитывающих широкий диапазон угроз.

ИБ достигается посредством внедрения соответствующих мер обеспечения ИБ, определенных в ходе выбранного процесса менеджмента рисков и управляемых с помощью СМИБ. Данные меры охватывают политику, процессы, процедуры, организационные структуры, программное и аппаратное обеспечение и предназначены для защиты идентифицированных информационных активов. Меры обеспечения информационной безопасности необходимо определить, внедрить, проверить, проанализировать и при необходимости улучшить, чтобы гарантировать соответствие уровня ИБ бизнес-целям организации. Меры обеспечения ИБ должны быть интегрированы в бизнес-процессы организации.

4.2.4 Менеджмент

Менеджмент включает в себя действия по управлению организацией, ее контролю и непрерывному совершенствованию в рамках соответствующих структур. Менеджмент охватывает действия, методы или практики формирования и обработки ресурсов, обращения с ресурсами, наблюдения за ними, а также управления ими. Масштаб управленческой структуры варьируется от одного человека в небольших организациях до управленческой иерархии, состоящей из многих людей, в крупных организациях.

Применительно к СМИБ менеджмент включает в себя наблюдение и принятие решений, необходимых для достижения бизнес-целей посредством защиты информационных активов организации. Менеджмент ИБ выражается через формулирование и использование политик ИБ, стандартов, процедур и рекомендаций, которые применяются повсеместно в организации всеми лицами, связанными с ней.

4.2.5 Система менеджмента

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

В части ИБ система менеджмента позволяет организации:

a) удовлетворять требования безопасности потребителей и других заинтересованных сторон;

b) совершенствовать планы и деятельность организации;

c) обеспечивать соответствие целям ИБ организации;

d) соответствовать требованиям регулирующих и законодательных органов, а также отраслевым нормативным документам;

e) управлять информационными активами системным образом, чтобы упростить процессы непрерывного совершенствования и регулирования текущих организационных целей.

4.3 Процессный подход

Чтобы оптимизировать свою деятельность, организация должна проводить различные виды мероприятий и управлять ими. Любое контролируемое мероприятие, использующее ресурсы в целях преобразования исходных данных в результаты, можно считать процессом. Результат одного процесса может непосредственно формировать исходные данные для следующего процесса. Обычно подобное преобразование происходит в условиях планирования и управления. Применение в рамках организации системы процессов, наряду с их идентификацией, обеспечением взаимодействия, а также управлением ими, можно назвать «процессным подходом».

4.4 Важность внедрения СМИБ

В рамках СМИБ организация должна выявить риски, связанные со своими информационными активами. Чтобы обеспечить ИБ, необходимо управлять рисками и учитывать относящиеся к угрозам физические, человеческие и технологические риски, применимые к любым формам информации внутри организации или используемые ею.

Внедрение СМИБ является стратегическим решением для организации. Необходимо сделать эту систему неотъемлемой частью организационной структуры организации, постоянно оценивать и обновлять в соответствии с текущими потребностями.

На разработку и внедрение СМИБ влияют задачи, цели, размер и структура организации, требования безопасности и используемые бизнес-процессы. Разработка и функционирование СМИБ должны отражать интересы и требования ИБ всех заинтересованных сторон организации, включая клиентов, поставщиков, деловых партнеров, акционеров и других третьих лиц.

Во взаимосвязанном мире информация и относящиеся к ней процессы, системы и сети составляют критически важные бизнес-активы. Организации, а также их информационные системы и сети сталкиваются с угрозами безопасности из широкого диапазона источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, а также пожар и наводнение. Повреждения информационных систем и сетей, вызванные вредоносным кодом, действиями хакеров и компьютерных атак типа «отказ в обслуживании», становятся более распространенными и более масштабными, а сами компьютерные атаки — все более изощренными.

СМИБ имеет огромную важность как для государственного, так и для частного секторов бизнеса. В любой отрасли СМИБ является фактором, способствующим поддержке электронного бизнеса, а также важным компонентом мероприятий по управлению рисками. Взаимодействие общедоступных и частных сетей, а также совместное использование информационных активов повышают сложность управления доступом к информации и ее обработкой. Кроме того, широкое использование мобильных устройств хранения данных, на которые записываются информационные активы, способно ослабить эффективность традиционных средств управления. Когда организация внедряет семейство стандартов СМИБ, она может продемонстрировать деловым партнерам и другим заинтересованным сторонам свою способность последовательно применять широко известные принципы ИБ.

При проектировании и разработке информационных систем не всегда учитываются аспекты ИБ. Кроме того, ИБ зачастую считают сугубо технической задачей. Однако уровень безопасности, достигаемый с помощью технических средств, недостаточно высок. Подобная защита может быть неэффективной, не будучи поддерживаемой соответствующими мерами обеспечения ИБ и процедурами в контексте СМИБ. Последующее встраивание системы безопасности в информационную систему бывает трудным и дорогостоящим. СМИБ включает в себя идентификацию имеющихся мер обеспечения ИБ и требует тщательного планирования и внимания к деталям. Например, средства управления доступом, которые могут быть техническими (логическими), физическими, административными (организационными) или их комбинацией, гарантируют, что доступ к информационным активам разрешен, но ограничен на основании потребностей бизнеса и требований безопасности.

Внедрение СМИБ имеет большое значение для защиты информационных активов, позволяя организации:

a) повысить гарантии того, что ее информационные активы в достаточной мере и на постоянной основе защищены от угроз ИБ;

b) поддерживать структурированную и всестороннюю систему идентификации и оценки угроз ИБ, выбора и применения соответствующих мер обеспечения ИБ, измерения и улучшения их эффективности;

c) непрерывно улучшать среду средств управления;

d) обеспечивать соответствие нормативным и регулятивным требованиям.

4.5 Разработка, мониторинг, поддержка и улучшение СМИБ

4.5.1 Общие сведения

Организация должна предпринимать следующие шаги по разработке, мониторингу, поддержке и улучшению своей СМИБ:

a) определение информационных активов и связанных с ними требований ИБ (см. 4.5.2);

b) оценка рисков ИБ (см. 4.5.3) и их обработка (см. 4.5.4);

c) выбор и внедрение соответствующих мер обеспечения ИБ в отношении неприемлемых рисков (см. 4.5.5);

d) мониторинг, поддержка и повышение эффективности мер обеспечения информационной безопасности, связанных с информационными активами организации (см. 4.5.6).

Для гарантии эффективной непрерывной защиты информационных активов организации с помощью СМИБ необходимо постоянно повторять шаги a) — d), чтобы выявлять изменения в рисках, стратегии организации или бизнес-целях.

4.5.2 Определение требований информационной безопасности

В рамках общей стратегии и бизнес-целей организации, ее размера и географического расположения требования ИБ можно сформулировать на основе анализа следующих факторов:

a) идентифицированные информационные активы и их ценность;

b) потребности бизнеса в обработке, обмене и хранении информации;

c) юридические, нормативные и договорные требования.

Проведение систематической оценки рисков, связанных с информационными активами организации, включает в себя анализы угроз информационным активам, уязвимостей и вероятности возникновения угрозы информационным активам, а также анализ потенциального воздействия любого инцидента ИБ на информационные активы. Расходы на соответствующие меры обеспечения ИБ будут пропорциональны предполагаемому влиянию риска на бизнес.

4.5.3 Оценка рисков информационной безопасности

Менеджмент риска ИБ требует должной оценки риска и метода его обработки. Это в свою очередь предполагает оценку затрат и преимуществ, законных требований, социальных, экономических и экологических аспектов, проблем заинтересованных сторон, приоритетов и других входных данных и переменных.

Оценка рисков должна выявлять, количественно оценивать и приоритизировать риски в сопоставлении с критериями принятия рисков и целями, представляющими важность для организации. Результаты оценки должны служить ориентиром и определять соответствующие управленческие меры и приоритеты для управления рисками ИБ и для внедрения мер обеспечения ИБ, выбранных для защиты от этих рисков.

Оценка риска должна включать в себя:

- систематический подход к оценке величины рисков (анализ рисков);
- процесс сравнения оцениваемых рисков с критериями риска для определения значимости рисков (оценка рисков).

Оценку рисков следует проводить регулярно, чтобы учитывать новые требования к ИБ, следить за ситуацией с рисками, например, в отношении активов, угроз, уязвимостей, воздействий, оценки рисков, а также в случае существенных изменений требований к ИБ. Такая оценка должна осуществляться по специальной методике, обеспечивающей сопоставимые и воспроизводимые результаты.

Чтобы оценка рисков ИБ была эффективной, она должна иметь четко определенную область применения и, при необходимости, проводиться совместно с оценкой рисков в других областях.

ИСО/МЭК 27005 предоставляет рекомендации по менеджменту рисков ИБ, в том числе по оценке, обработке, принятию, мониторингу и проверке рисков, а также по связанным с рисками коммуникациям. Он также содержит примеры методик оценки рисков.

4.5.4 Обработка рисков информационной безопасности

Прежде чем рассматривать вопрос, связанный с обработкой риска, организация должна определить критерии, устанавливающие возможность принятия или непринятия риска. Риск может быть принят, если, например, определено, что он невысок, или не принят, если стоимость его обработки экономически нецелесообразна для организации. Такие решения следует задокументировать.

После оценки рисков необходимо принять решение об их обработке. Ниже перечислены возможные подходы к обработке рисков:

a) применить соответствующие меры обеспечения ИБ, позволяющие снизить риски;

b) сознательно и объективно принять риски при условии, что они четко соответствуют политике организации и критериям такого принятия;

c) избегать рисков путем запрета действий, которые могут привести к возникновению рисков;

d) распределить риски с другими сторонами, например, со страховщиками или поставщиками.

По тем рискам, в отношении которых было решено применить меры обеспечения ИБ, необходимо выбрать соответствующие меры и внедрить их.

4.5.5 Выбор и внедрение мер обеспечения информационной безопасности

После определения требований ИБ (см. 4.5.2), определения и оценки рисков ИБ для выявленных информационных активов (см. 4.5.3) и принятия решений по обработке рисков (см. 4.5.4) необходимо выбрать и внедрить меры обеспечения ИБ для снижения рисков.

Применяемые меры обеспечения ИБ должны способствовать снижению рисков до приемлемого уровня исходя из:

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

b) целей организации;

c) эксплуатационных требований и ограничений;

d) стоимости их внедрения и эксплуатации с учетом снижения рисков при сохранении соразмерности требованиям и ограничениям организации;

e) задач по мониторингу, оценке и повышению эффективности и действенности мер обеспечения ИБ в соответствии с целями организации. Выбор и внедрение соответствующих мер обеспечения ИБ необходимо задокументировать в рамках заявления о применимости, чтобы обеспечить соблюдение требований;

f) необходимости обеспечения баланса между инвестициями во внедрение и поддержку мер обеспечения ИБ и потерями, возможными в результате инцидентов ИБ.

Меры обеспечения ИБ, приведенные в ИСО/МЭК 27002, признаны передовой практикой, применимой к большинству организаций, и легко адаптируются к организациям различного размера и сложности. Другие стандарты из семейства стандартов СМИБ предоставляют рекомендации по выбору и применению мер обеспечения ИБ из ИСО/МЭК 27002 для СМИБ.

Меры обеспечения ИБ необходимо учитывать на этапе разработки требований к проектам и системам. В противном случае это может увеличить затраты и снизить эффективность решений, а в худшем случае — сделать невозможным достижение адекватного уровня безопасности. Меры обеспечения информационной безопасности могут быть выбраны из ИСО/МЭК 27002 или из числа других подходящих наборов мер обеспечения ИБ. Кроме того, для удовлетворения конкретных потребностей организации могут быть разработаны новые специальные меры обеспечения ИБ. Необходимо признать, что не все меры обеспечения информационной безопасности подходят для применения в информационных системах или средах и практической реализации во всех организациях.

В отдельных случаях для внедрения выбранного набора мер обеспечения ИБ требуется время, и в течение этого времени уровень риска может быть выше допустимого в долгосрочной перспективе. Критерии риска должны охватывать допустимость рисков в краткосрочной перспективе, в период реализации мер обеспечения ИБ. Следует проинформировать заинтересованные стороны об уровнях риска, которые оцениваются и ожидаются в различные моменты времени, по мере постепенного внедрения данных мер обеспечения информационной безопасности.

Следует учитывать, что ни один набор мер обеспечения ИБ не может гарантировать полную ИБ. Необходимо внедрить дополнительные управленческие меры по мониторингу, оценке и повышению эффективности и действенности мер обеспечения ИБ в соответствии с целями организации.

Выбор и внедрение мер обеспечения информационной безопасности должны быть задокументированы в заявлении о применимости, чтобы обеспечить соблюдение требований.

4.5.6 Мониторинг, поддержка и повышение эффективности СМИБ

Организация должна поддерживать работоспособность и улучшать СМИБ посредством мониторинга и оценки эффективности в соответствии с политикой и целями организации, а также информировать руководство о полученных результатах для проверки. Цель такой проверки — удостовериться, что СМИБ включает в себя определенные меры обеспечения ИБ, применимые для обработки охватываемых ею рисков. Кроме того, на основе отчетов об этих областях мониторинга можно получить доказательства проверки и отслеживания корректирующих и предупреждающих мер, а также мер по улучшению ситуации.

4.5.7 Постоянное улучшение

Основной целью постоянного улучшения СМИБ является повышение вероятности достижения целей, связанных с сохранением конфиденциальности, доступности и целостности информации. Основной задачей в этой сфере является поиск путей для совершенствования; не следует думать, что используемая практика управления ИБ достаточна или максимально эффективна.

Мероприятия по улучшению:

a) анализ и оценка существующей ситуации для выявления областей, нуждающихся в совершенствовании;

b) постановка задач по совершенствованию;

c) поиск возможных решений для достижения поставленных целей;

d) оценка этих решений и выбор;

e) внедрение выбранного решения;

f) измерение, верификация, анализ и оценка результатов внедрения, чтобы определить, насколько достигнуты поставленные цели;

g) официальное оформление изменений.

Полученные результаты перепроверяют по мере необходимости, чтобы наметить дальнейшие пути улучшения. Таким образом, улучшение является непрерывным процессом, т. е. действия повторяются с определенной частотой. Чтобы выявлять возможности улучшения, можно также использовать отзывы клиентов и других заинтересованных сторон, результаты аудитов и проверок СМИБ.

4.6 Важнейшие факторы успешной реализации СМИБ

Чтобы успешно внедрить СМИБ и таким образом решить поставленные бизнес-задачи, следует учесть множество критически важных факторов. Примеры важнейших факторов успеха:

a) политика ИБ, цели и действия, ориентированные на решение поставленных задач;

b) методика и структура для разработки, внедрения, мониторинга, поддержки и улучшения ИБ, согласующиеся с корпоративной культурой;

c) значительная поддержка и заинтересованность со стороны всех уровней управления, в особенности высшего руководства;

d) понимание требований информационной защиты активов, достигаемое через применение менеджмента рисков ИБ (см. ИСО/МЭК 27005);

e) эффективное просвещение персонала и других причастных сторон по вопросам ИБ, проведение тренингов и обучающих программ, доведение до сведения сотрудников их обязательств в сфере ИБ, сформулированных в политике ИБ, информации о стандартах и т. д., а также мотивирование сотрудников к соответствующим действиям;

f) эффективный процесс управления инцидентами ИБ;

g) эффективный управленческий подход к обеспечению непрерывности бизнеса;

h) использование системы измерения, позволяющей оценивать управление ИБ;

i) поступление предложений по улучшению в формате обратной связи.

СМИБ увеличивает вероятность того, что организация будет последовательно реализовывать важнейшие факторы успеха, необходимые для защиты ее информационных активов.

4.7 Преимущества применения семейства стандартов СМИБ

Преимущества внедрения СМИБ вытекают прежде всего из сокращения рисков ИБ (то есть уменьшения вероятности воздействия и/или уменьшения воздействия, вызванного инцидентами ИБ). В частности, преимуществами, полученными от принятия семейства стандартов СМИБ, являются:

a) структурированная поддержка процесса определения, внедрения, функционирования и поддержания работоспособности полной и экономически эффективной комплексной СМИБ, которая создает ценность и удовлетворяет потребности организации в рамках различных операций и на различных объектах;

b) помощь руководителям в применении системного подхода к менеджменту ИБ в контексте корпоративного управления рисками и общего руководства, в том числе тренинги и обучение представителей бизнеса и владельцев СМИБ унифицированному подходу к менеджменту ИБ;

c) продвижение общепринятых передовых практик ИБ в недирективной форме (это предоставляет организации свободу в использовании и улучшении мер обеспечения ИБ, которые отвечают ее специфическим требованиям и помогают решать проблемы, возникающие как внутри организации, так и за ее пределами);

d) предоставление общего языка и концептуальной основы для обеспечения ИБ (это способствует взаимопониманию с деловыми партнерами, особенно если они требуют наличия сертификата соответствия ИСО/МЭК 27001 от аккредитованного органа сертификации);

e) повышение доверия заинтересованных сторон к организации;

f) удовлетворение потребностей и ожиданий общества;

g) более эффективное с экономической точки зрения управление инвестициями в ИБ.

5 Семейство стандартов СМИБ

5.1 Общая информация

Семейство стандартов СМИБ состоит из взаимосвязанных стандартов, опубликованных или разрабатываемых, и содержит несколько ключевых структурных компонентов. К числу этих компонентов относятся:

- нормативные стандарты, устанавливающие требования к СМИБ (ИСО/МЭК 27001);
- требования к органам по сертификации, осуществляющим сертификацию на соответствие ИСО/МЭК 27001 (ИСО/МЭК 27006);
- дополнительные требования, связанные с внедрением СМИБ в конкретных отраслях (ИСО/МЭК 27009).

Другие стандарты предоставляют рекомендации по различным аспектам внедрения СМИБ, в том числе по общему процессу и управлению, а также специальные руководства для конкретных отраслей.

Взаимосвязи в семействе стандартов СМИБ приведены на рисунке 1.

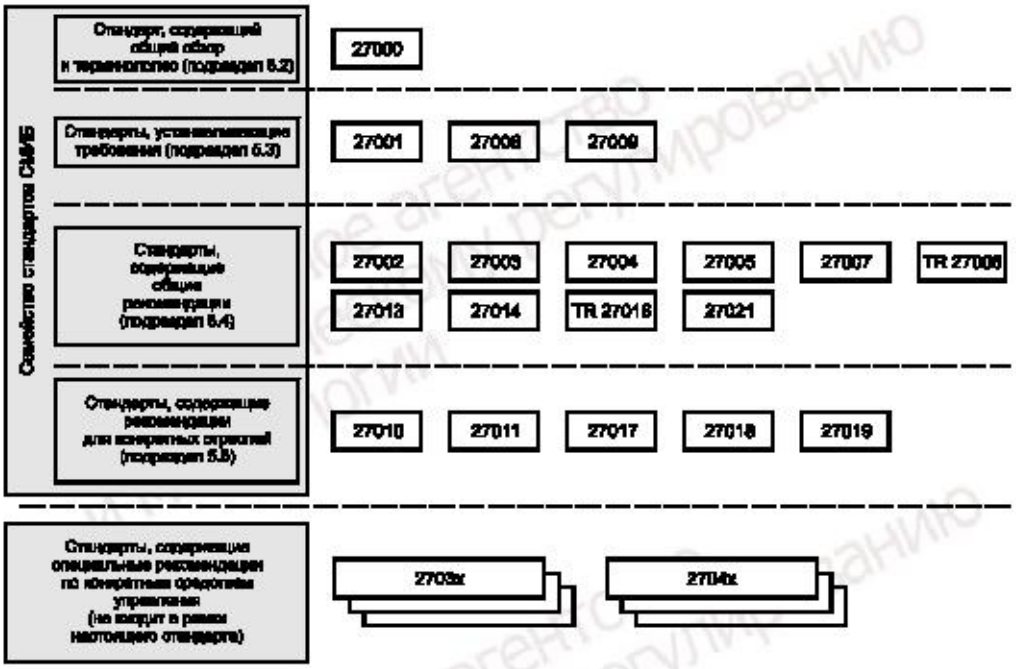

Рисунок 1 — Взаимосвязи в семействе стандартов СМИБ

Каждый стандарт из семейства стандартов СМИБ описывается ниже в соответствии с его назначением (или ролью) в этом семействе и идентификационным номером.

5.2 Стандарт, содержащий общий обзор и терминологию: ИСО/МЭК 27000 (настоящий стандарт)

ИСО/МЭК 27000 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (Information technology — Security techniques — Information security management systems — Overview and vocabulary)

Область применения. Настоящий стандарт содержит:

a) обзор семейства стандартов СМИБ;

b) введение в систему менеджмента ИБ;

c) термины и определения для использования в семействе стандартов СМИБ.

Назначение. Настоящий стандарт описывает основы системы менеджмента информационной безопасности, которые составляют предмет семейства стандартов СМИБ, а также определяет относящиеся к СМИБ термины.

5.3 Стандарты, устанавливающие требования

5.3.1 ИСО/МЭК 27001

ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (Information technology — Security techniques — Information security management systems — Requirements)

Область применения. ИСО/МЭК 27001 определяет требования к разработке, внедрению, эксплуатации, мониторингу, анализу, поддержке в рабочем состоянии и улучшению задокументированной СМИБ в контексте общих бизнес-рисков организации. Он устанавливает требования к внедрению мер

обеспечения ИБ с учетом задач отдельных организаций или их подразделений. Данный стандарт применим к организациям любого типа, масштаба и сферы деятельности.

Назначение. ИСО/МЭК 27001 содержит нормативные требования к реализации и функционированию СМИБ, в том числе описывает меры обеспечения ИБ, позволяющие контролировать и снижать риски в отношении информационных активов, которые организация стремится защитить. Организации, использующие СМИБ, могут проводить ее аудиторскую проверку и сертификацию соответствия. В целях удовлетворения выявленных требований необходимо выбрать цели и меры обеспечения ИБ из приложения А ИСО/МЭК 27001:2013 в качестве компонента СМИБ-процесса. Цели и меры обеспечения ИБ, приведенные в таблице А.1 ИСО/МЭК 27001:2013, выбраны непосредственно из списка целей и мер обеспечения ИБ, содержащихся в разделах 5—18 ИСО/МЭК 27001:2013, и согласованы с ними.

5.3.2 ИСО/МЭК 27006

ИСО/МЭК 27006 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности» (Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems)

Область применения. ИСО/МЭК 27006 содержит список требований и рекомендаций для органов, осуществляющих аудит и сертификацию СМИБ на соответствие ИСО/МЭК 27001 (в дополнение к требованиям ИСО/МЭК 17021). Данный стандарт предназначен главным образом для аккредитации органов, осуществляющих сертификацию СМИБ на соответствие ИСО/МЭК 27001.

В ИСО/МЭК 27001 приведены требования к компетентности и надежности, выполнение которых должно продемонстрировать любое лицо, осуществляющее сертификацию СМИБ, а также предназначенные для этого лица рекомендации, подробно разъясняющие данные требования.

Назначение. ИСО/МЭК 27006 дополняет ИСО/МЭК 17021 в части требований для аккредитации органов сертификации, осуществляющих сертификацию соответствия требованиям, установленным в ИСО/МЭК 27001.

5.3.3 ИСО/МЭК 27009

ИСО/МЭК 27009 «Информационные технологии. Методы и средства обеспечения безопасности. Специфическое для отраслей экономики применение ИСО/МЭК 27001. Требования» (Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements)[1)]

Область применения. ИСО/МЭК 27009 устанавливает требования к использованию ИСО/МЭК 27001 в конкретных секторах (определенных отраслях, областях практического применения или в рыночном секторе). В нем даются разъяснения, как расширить ИСО/МЭК 27001 дополнительными требованиями и усовершенствовать требования ИСО/МЭК 27001, а также о включении в приложение А ИСО/МЭК 27001:2013 дополнительных мер и средств (наборов средств) обеспечения ИБ.

Назначение. ИСО/МЭК 27009 обеспечивает соответствие дополнительных или уточненных требований положениям ИСО/МЭК 27001.

5.4 Стандарты, содержащие общие рекомендации

5.4.1 ИСО/МЭК 27002

ИСО/МЭК 27002 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности» (Information technology — Security techniques — Code of practice for information security controls)

Область применения. ИСО/МЭК 27002 содержит перечень общепринятых мер обеспечения ИБ и передовые практики реализации соответствующих мер, которые можно использовать в качестве рекомендаций по выбору и внедрению мер обеспечения ИБ.

Назначение. ИСО/МЭК 27002 предоставляет рекомендации по внедрению мер обеспечения ИБ. В частности, в разделах 5—18 приведены специальные рекомендации, а также инструкции по применению передовых практик для поддержки мер обеспечения ИБ, указанных в разделах А.5—А.18 ИСО/МЭК 27001.

5.4.2 ИСО/МЭК 27003

ИСО/МЭК 27003 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство» (Information technology — Security techniques — Information security management systems — Guidance)

[1)] *Заменен на ISO/IEC 27009:2020.*

Область применения. ИСО/МЭК 27003 содержит разъяснения и практические рекомендации по внедрению ИСО/МЭК 27001.

Назначение. ИСО/МЭК 27003 содержит описание процессного подхода к внедрению СМИБ в соответствии с ИСО/МЭК 27001.

5.4.3 ИСО/МЭК 27004

ИСО/МЭК 27004 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание» (Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation)

Область применения. ИСО/МЭК 27004 содержит рекомендации, призванные помочь организациям в оценке деятельности по обеспечению ИБ и эффективности СМИБ в целях выполнения требований ИСО/МЭК 27001:2013, подраздел 9.1. В нем рассматриваются:

a) мониторинг и оценка действенности информационной безопасности;

b) мониторинг и оценка эффективности системы менеджмента информационной безопасности (СМИБ), включая ее процессы и средства контроля и управления;

c) анализ и оценка результатов мониторинга и оценки защищенности.

Назначение. ИСО/МЭК 27004 предоставляет систему измерений, позволяющую оценивать эффективность СМИБ в соответствии с ИСО/МЭК 27001.

5.4.4 ИСО/МЭК 27005

ИСО/МЭК 27005 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (Information technology — Security techniques — Information security risk management)

Область применения. ИСО/МЭК 27005 содержит рекомендации по менеджменту рисков ИБ. Подход, принятый в данном стандарте, соответствует общим принципам, изложенным в ИСО/МЭК 27001.

Назначение. ИСО/МЭК 27005 содержит рекомендации по внедрению процессного подхода к менеджменту рисков, позволяющего обеспечить полное выполнение требований ИСО/МЭК 27001, относящихся к менеджменту рисков ИБ.

5.4.5 ИСО/МЭК 27007

ИСО/МЭК 27007 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по аудиту систем менеджмента информационной безопасности» (Information technology — Security techniques — Guidelines for information security management systems auditing)[1)]

Область применения. ИСО/МЭК 27007 содержит рекомендации по проведению аудитов СМИБ и оценке компетентности аудиторов СМИБ, дополняющие рекомендации, приведенные в ИСО 19011, который относится к системам менеджмента в целом.

Назначение. В ИСО/МЭК 27007 приведены рекомендации для организаций, которым необходимо проводить внутренние или внешние аудиты СМИБ или управлять программой проведения аудита СМИБ в соответствии с требованиями ИСО/МЭК 27001.

5.4.6 ИСО/МЭК ТО 27008

ИСО/МЭК ТО 27008 «Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации для аудиторов по оценке мер обеспечения информационной безопасности» (Information technology — Security techniques — Guidelines for auditors on information security controls)[2)]

Область применения. В ИСО/МЭК ТО 27008 содержатся рекомендации по проверке внедрения и оценке мер обеспечения информационной безопасности, включая проверку технического соответствия средств управления информационных систем, в соответствии с используемыми в организации стандартами СМИБ.

Назначение. В настоящем техническом отчете основное внимание уделяется проверке мер обеспечения ИБ, включая проверку технического соответствия в контексте внедренного организацией стандарта СМИБ. В данном документе отсутствуют конкретные указания по проверке соответствия, связанной с измерением, оценкой рисков или аудитом СМИБ, как указано в ИСО/МЭК 27004, ИСО/МЭК 27005 или ИСО/МЭК 27007 соответственно. Технический отчет не предназначен для аудитов систем менеджмента.

[1)] *Заменен на ISO/IEC 27007:2020.*

[2)] *Заменен на ISO/IEC TS 27008:2019.*

5.4.7 ИСО/МЭК 27013

ИСО/МЭК 27013 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1» (Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1).

Область применения. ИСО/МЭК 27013 содержит рекомендации по комплексному внедрению ИСО/МЭК 27001 и ИСО/МЭК 20000-1 в организациях, которые намереваются:

a) внедрить ИСО/МЭК 27001 после внедрения ИСО/МЭК 20000-1 или наоборот;

b) совместно использовать ИСО/МЭК 27001 и ИСО/МЭК 20000-1;

c) интегрировать существующие системы менеджмента, основанные на ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

Основное внимание в данном стандарте уделено исключительно комплексной реализации СМИБ, как указано в ИСО/МЭК 27001, и системы управления услугами (СУУ), как указано в ИСО/МЭК 20000-1.

Кроме того, на практике ИСО/МЭК 27001 и ИСО/МЭК 20000-1 могут быть интегрированы с другими стандартами системы менеджмента, например, с ИСО 9001 и ИСО 14001.

Назначение. Целью данного стандарта является предоставление организациям подобного разъяснения характеристик, сходства и различий ИСО/МЭК 27001 и ИСО/МЭК 20000-1, чтобы помочь спланировать интегрированную систему менеджмента, соответствующую каждому их этих стандартов.

5.4.8 ИСО/МЭК 27014

ИСО/МЭК 27014 «Информационные технологии. Методы и средства обеспечения безопасности. Руководство деятельностью по обеспечению информационной безопасности» (Information technology — Security techniques — Governance of information security)[1)]

Область применения. В ИСО/МЭК 27014 представлены рекомендации относительно принципов и процессов управления ИБ, с помощью которых организации смогут оценивать, руководить и контролировать сферу менеджмента ИБ.

Назначение. Обеспечение ИБ становится важнейшей задачей для организаций. Не только усиление нормативных требований, но и несовершенство мер обеспечения ИБ могут непосредственно влиять на репутацию организации. Поэтому руководящим органам в рамках своих обязанностей все чаще приходится осуществлять надзор за ИБ, чтобы помочь организациям в достижении целей в этой области.

5.4.9 ИСО/МЭК ТО 27016

ИСО/МЭК ТО 27016 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Организационная экономика» (Information technology — Security techniques — Information security management — Organizational economics)

Область применения. В данном техническом отчете излагается методология, позволяющая организациям лучше понять, каким образом более точно оценивать свои информационные активы, анализировать потенциальные риски для этих активов, определять важность мер обеспечения ИБ и оптимальный уровень ресурсов, используемых для обеспечения безопасности этих информационных активов.

Назначение. Данный технический отчет дополняет семейство стандартов СМИБ, охватывая экономический аспект защиты информационных активов организации в контексте более широкой социальной среды, в которой действует организация, и предоставляет рекомендации по применению организационной экономики ИБ посредством соответствующих моделей и практических примеров.

5.4.10 ИСО/МЭК 27021

ИСО/МЭК 27021 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности» (Information technology — Security techniques — Competence requirements for information security management systems professionals)

Область применения. ИСО/МЭК 27021 определяет требования к компетентности специалистов в области СМИБ, руководящих созданием, внедрением, поддержкой и постоянным совершенствованием одного или нескольких процессов СМИБ, соответствующей ИСО/МЭК 27001:2013, либо участвующих в подобной деятельности.

Назначение. Данный стандарт предназначен для использования:

[1)] *Заменен на ISO/IEC 27014:2020.*

a) лицами, которые стремятся продемонстрировать свою компетентность в качестве специалистов по СМИБ или хотят развить навыки, необходимые для работы в этой области, или желают углубить свои знания;

b) организациями, заинтересованными в поиске потенциальных квалифицированных кандидатов на должности, связанные со СМИБ, для определения компетентности, необходимой для этих должностей;

c) органами по разработке процедур сертификации специалистов в области СМИБ, которым необходим свод знаний для формирования источников экспертных знаний;

d) организациями в сфере образования и профессиональной подготовки, такими как университеты и профессиональные учебные заведения, с целью приведения учебных планов и курсов в соответствие с требованиями к компетентности специалистов в области СМИБ.

5.5 Стандарты, содержащие рекомендации для конкретных отраслей

5.5.1 ИСО/МЭК 27010

ИСО/МЭК 27010 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности при обмене информацией между отраслями и организациями» (Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications)

Область применения. ИСО/МЭК 27010 содержит рекомендации, которые дополняют рекомендации из семейства стандартов ИСО/МЭК 27000 и относятся к внедрению СМИБ в рамках информационного обмена между сообществами.

Данный стандарт описывает меры обеспечения информационной безопасности и предоставляет рекомендации, касающиеся инициирования, внедрения, поддержки и повышения уровня ИБ в рамках информационного обмена между отраслями и организациями.

Назначение. Данный стандарт применим ко всем формам обмена и совместного использования конфиденциальной информации, как государственной, так и частной, на национальном и международном уровнях, в рамках одной и той же отрасли, или сектора рынка, или между секторами. В частности, он применим к обмену информацией и совместному использованию информации, связанной с предоставлением, обслуживанием и защитой критических объектов инфраструктуры на уровне организации или государства.

5.5.2 ИСО/МЭК 27011

ИСО/МЭК 27011 «Информационные технологии. Методы и средства обеспечения безопасности. Практическое руководство по обеспечению информационной безопасности организаций, предлагающих телекоммуникационные услуги, на основе ИСО/МЭК 27002» (Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations)

Область применения. ИСО/МЭК 27011 содержит рекомендации по внедрению мер обеспечения ИБ в телекоммуникационных организациях.

Назначение. ИСО/МЭК 27011 предоставляет телекоммуникационным организациям возможность соблюдать базовые требования к менеджменту ИБ в отношении конфиденциальности, целостности, доступности и иных подлежащих защите аспектов.

5.5.3 ИСО/МЭК 27017

ИСО/МЭК 27017 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб» (Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services)

Область применения. В ИСО/МЭК 27017 приведены рекомендации по управлению ИБ, применимые к мерам обеспечения ИБ при использовании облачных служб благодаря:

- предоставлению дополнительных рекомендаций по внедрению соответствующих мер обеспечения ИБ, приведенных в ИСО/МЭК 27002;
- предоставлению дополнительных мер обеспечения ИБ и соответствующих рекомендаций по внедрению, относящихся конкретно к облачным службам.

Назначение. В ИСО/МЭК 27017 приведены рекомендации по реализации мер обеспечения ИБ как для потребителей, так и для поставщиков облачных служб.

5.5.4 ИСО/МЭК 27018

ИСО/МЭК 27018 «Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки» (Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

Область применения. ИСО/МЭК 27018 определяет общие задачи и меры обеспечения ИБ, а также предоставляет рекомендации, связанные с внедрением мер по защите персональных данных (ПДн) в соответствии с принципами конфиденциальности, приведенными в ИСО/МЭК 29100, для публичной облачной среды.

Назначение. Данный стандарт применим к организациям, включая государственные организации и частные компании, правительственные учреждения и некоммерческие организации, которые предоставляют услуги по обработке информации в качестве обработчиков ПДн в облачных средах по контракту с другими организациями. Рекомендации, содержащиеся в этом стандарте, также могут использовать организации, выступающие в качестве операторов персональных данных. Однако на операторов ПДн могут распространяться дополнительные законодательные и нормативные акты и обязательства по защите ПДн, не относящиеся к обработчикам ПДн, они в данном стандарте не рассматриваются.

5.5.5 ИСО/МЭК 27019

ИСО/МЭК 27019 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности энергосистем общего пользования» (Information technology — Security techniques — Information security controls for the energy utility industry)

Область применения. ИСО/МЭК 27019 содержит рекомендации, основанные на ИСО/МЭК 27002:2013, который применим к системам управления технологическими процессами, используемыми в энергетике для контроля и мониторинга производства, передачи, хранения и распределения электроэнергии, газа, нефти и тепловой энергии, а также для управления соответствующими вспомогательными процессами. В частности, к ним относится использование:

- централизованного и распределенного управления технологическими процессами, технологии контроля и автоматизации, а также информационных систем, применяемых для их эксплуатации, таких как устройства программирования и параметризации;
- цифровых контроллеров и компонентов автоматизации, таких как устройства управления и периферийные устройства или программируемые логические контроллеры (ПЛК), включая цифровые датчики и приводные элементы;
- любых дополнительных поддерживающих информационных систем, применяемых для управления технологическими процессами, например, для выполнения дополнительных задач визуализации данных, а также для управления, мониторинга, архивирования данных, ведения журналов учета, составления отчетов и документирования;
- коммуникационной технологии в области управления технологическими процессами, например, сетей, телеметрии, телекоммуникационных приложений и технологии дистанционного управления;
- компонентов развитой измерительной инфраструктуры (Advanced Metering Infrastructure, AMI), например, интеллектуальных счетчиков;
- измерительных устройств, например, для определения уровня выбросов;
- цифровых систем защиты и безопасности, например, защитных реле, ПЛК безопасности, аварийных механизмов управления;
- систем управления энергоснабжением, например, систем распределенных энергетических ресурсов (РЭР), инфраструктуры электрозарядки, в частных домах, жилых зданиях или промышленных установках потребителей;
- распределенных компонентов интеллектуальных сетей, например, в энергетических сетях, в частных домах, жилых зданиях или промышленных установках потребителей;
- любого программного обеспечения, встроенного программного обеспечения и приложений, установленных на вышеуказанных системах, например, приложений систем управления дистрибуцией (distribution management system, DMS) или систем управления отключениями (outage management system, OMS);
- любых помещений, в которых размещено вышеуказанное оборудование и системы;
- систем дистанционного обслуживания для вышеупомянутых систем.

ИСО/МЭК 27019 не относится к области контроля технологических процессов на ядерных установках. Данная область подпадает под действие МЭК 62645.

ИСО/МЭК 27019 также включает требование по проведению процессов оценки и обработки рисков, описанных в ИСО/МЭК 27001:2013, в соответствии с инструкциями, представленными в данном стандарте для конкретного сектора энергетического хозяйства.

Назначение. В дополнение к целям и мерам обеспечения ИБ, изложенным в ИСО/МЭК 27002, данный стандарт содержит рекомендации для СМИБ, используемых энергетическими компаниями и поставщиками энергоресурсов и учитывающих дополнительные специфические требования.

5.5.6 ИСО 27799

ИСО 27799 «Информатизация здоровья. Менеджмент защиты информации в здравоохранении по ИСО/МЭК 27002» (Health informatics — Information security management in health using ISO/IEC 27002)

Область применения. В данном стандарте приводятся рекомендации в отношении организационных стандартов СМИБ и практик управления ИБ, в том числе по выбору, внедрению и контролю мер обеспечения ИБ с учетом рисков ИБ организации.

ИСО 27799 предоставляет рекомендации по внедрению мер обеспечения ИБ, приведенные в ИСО/МЭК 27002, и при необходимости дополняет их с целью эффективного управления ИБ в сфере здравоохранения.

Назначение. ИСО 27799 предоставляет организациям здравоохранения рекомендации на основе ИСО/МЭК 27002 с учетом специфики данной отрасли и дополняет их требованиями, изложенными в ИСО/МЭК 27001:2013, приложение А.

Библиография

[1] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary

[2] ISO/IEC/IEEE 15939:2017, Systems and software engineering — Measurement process

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

[4] ISO 19011:2011, Guidelines for auditing management systems

[5] ISO/IEC 20000-1:2011, Information technology — Service management — Part 1: Service management system requirements

[6] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[7] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[8] ISO/IEC 27003, Information technology — Security techniques — Information security management systems — Guidance

[9] ISO/IEC 27004, Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

[10] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

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

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

[13] ISO/IEC TR 27008, Information technology — Security techniques — Guidelines for auditors on information security controls

[14] ISO/IEC 27009, Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements

[15] ISO/IEC 27010, Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

[16] ISO/IEC 27011, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

[17] ISO/IEC 27013, Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

[18] ISO/IEC 27014, Information technology — Security techniques — Governance of information security

[19] ISO/IEC TR 27016, Information technology — Security techniques — Information security management — Organizational economics

[20] ISO/IEC 27017, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[21] ISO/IEC 27018, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[22] ISO/IEC 27019, Information technology — Security techniques — Information security controls for the energy utility industry

[23] ISO/IEC 27021, Information technology — Security techniques — Competence requirements for information security management systems professionals

[24] ISO 27799, Health informatics — Information security management in health using ISO/IEC 27002

[25] ISO Guide 73:2009, Risk management — Vocabulary

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: информационная безопасность (ИБ), система менеджмента информационной безопасности (СМИБ), менеджмент риска, меры обеспечения информационной безопасности

Редактор *Н.Н. Кузьмина*
Технический редактор *И.Е. Черепкова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 25.05.2021. Подписано в печать 31.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru