ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27021— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Требования к компетентности специалистов по системам менеджмента информационной безопасности

(ISO/IEC 27021:2017, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) 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. № 390-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27021:2017 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетентности специалистов по системам менеджмента информационной безопасности» (ISO/IEC 27021:2017 «Information technology — Security techniques — Competence requirements for information security management systems professionals», IDT).

ИСО/МЭК 27021 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).

При применении настоящего стандарта рекомендуется использовать вместо ссылочного международного стандарта соответствующий ему национальный стандарт, сведения о котором приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (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

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения. 1
4 Концепция и структура 2
4.1 Общие сведения 2
4.2 Концепция компетентности СМИБ 2
4.3 Структура компетентности СМИБ 2
4.4 Демонстрация компетентности 3
4.5 Структура настоящего стандарта 3
5 Общепрофессиональные компетентности в области менеджмента бизнеса для СМИБ-специалистов 3
5.1 Общие сведения 3
5.2 Компетентность: руководство 4
5.3 Компетентность: взаимодействие 4
5.4 Компетентность: бизнес-стратегия и СМИБ 4
5.5 Компетентность: менеджмент создания организации, культуры, поведения и заинтересованных сторон 5
5.6 Компетентность: менеджмент проектирования процессов и изменений организации 5
5.7 Компетентность: кадровый менеджмент менеджмент коллективов и отдельных лиц 6
5.8 Компетентность: менеджмент рисков 6
5.9 Компетентность: менеджмент ресурсов 7
5.10 Компетентность: архитектура информационных систем 7
5.11 Компетентность: менеджмент проектов и портфеля проектов 7
5.12 Компетентность: менеджмент поставщиков 8
5.13 Компетентность: менеджмент проблем 8
6 Компетентности в области информационной безопасности для СМИБ-специалистов 8
6.1 СМИБ-компетентность: информационная безопасность 8
6.2 СМИБ-компетентность: планирование информационной безопасности 10
6.3 СМИБ-компетентность: функционирование информационной безопасности 11
6.4 СМИБ-компетентность: поддержка информационной безопасности 11
6.5 СМИБ-компетентность: оценка эффективности информационной безопасности 12
6.6 СМИБ-компетентность: улучшение информационной безопасности 14
Приложение А (справочное) Совокупность терминов, характеризующих необходимые знания для СМИБ-специалистов как часть свода знаний 16
Приложение ДА (справочное) Сведения о соответствии ссылочного международного стандарта национальному стандарту 22
Библиография 23

Введение

Настоящий стандарт предназначен для использования:

- лицами, которые хотели бы продемонстрировать свою компетентность в области менеджмента информационной безопасности;
- СМИБ-специалистами или специалистами, желающими понять и достичь требуемой компетентности для работы в этой сфере, а также желающими расширить свои знания;
- организациями, ищущими потенциальных кандидатов среди СМИБ-специалистов для определения требуемых от них компетентностей, необходимых для занятия должностей организаций, предполагающих выполнение ролей, связанных со СМИБ;
- органами по разработке программ сертификации СМИБ-специалистов, предназначенных для использования центрами сертификации при проведении мероприятий, связанных с проверкой уровня компетентности у СМИБ-специалистов;
- образовательными учреждениями (университетами, учреждениями дополнительного профессионального образования) для согласования их учебных планов и программ в соответствии с требованиями к компетентностям, которыми должны обладать их выпускники в области СМИБ.

Настоящий стандарт следует рассматривать и использовать в комплексе с ИСО/МЭК 27001[1)].

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт устанавливает требования к компетентности специалистов по системам менеджмента информационной безопасности (СМИБ-специалистов), выполняющих или участвующих в разработке, реализации, осуществлении контроля и постоянном совершенствовании одного или нескольких процессов менеджмента информационной безопасности, соответствующих ИСО/МЭК 27001.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт. Для датированной ссылки применяют только указанное издание, для недатированной — последнее издание (включая все изменения):

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности. Общий обзор и терминология)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, а также следующие термины с соответствующими определениями.

С целью использования в своих стандартах международные организации ИСО и МЭК поддерживают терминологические базы данных:

- платформа ИСО для онлайн-просмотра доступна по адресу http://www.iso.org/obp;
- платформа МЭК Электропедия (IEC Electropedia) доступна по адресу http://www.electropedia.org/.

3.1

компетентность (competence): Способность применять знания и навыки для достижения намеченных целей.

[ИСО/МЭК 17024:2012, статья 3.6]

3.2 **специалист по системам менеджмента информационной безопасности (СМИБ-специалист)** (information security management system professional, ISMS professional): Лицо, которое разрабатывает, реализует, осуществляет контроль и постоянно совершенствует один или несколько процессов системы менеджмента информационной безопасности.

Издание официальное

4 Концепция и структура

4.1 Общие сведения

СМИБ-специалисты — это специалисты (сотрудники), чья роль заключается в менеджменте, внедрении, сопровождении и постоянном совершенствовании одного или нескольких процессов системы менеджмента информационной безопасности. Для успешного выполнения своей роли они должны обладать знаниями, навыками, определенными в настоящем стандарте, и поддерживать их на соответствующем уровне.

4.2 Концепция компетентности СМИБ

Внутри организации могут быть внедрены, эксплуатироваться и обслуживаться несколько систем менеджмента. За каждую систему менеджмента отвечает один или несколько специалистов. Настоящий стандарт рассматривает каждую такую систему менеджмента (СМ) как систему, необходимую для менеджмента бизнес-процессов организации в определенной предметной области. При этом каждая СМ требует специалистов, компетентных в области менеджмента и обладающих компетентностями, относящимися и к менеджменту, а также к предметной области. В качестве примера на рисунке 1 показана связь общепрофессиональных компетентностей в области менеджмента и профессиональных компетентностей четырех предметных областей (А, В, Х, ИБ). Среди данных предметных областей имеется и область информационной безопасности. Исходя из этого в настоящем стандарте отдельно рассмотрены общепрофессиональные компетентности, относящиеся к менеджменту бизнес-процессов (см. раздел 5) и профессиональные компетентности, относящиеся к области СМИБ, которые учитывают первую группу компетентностей и компетентностей в области информационной безопасности (ИБ) (см. раздел 6).

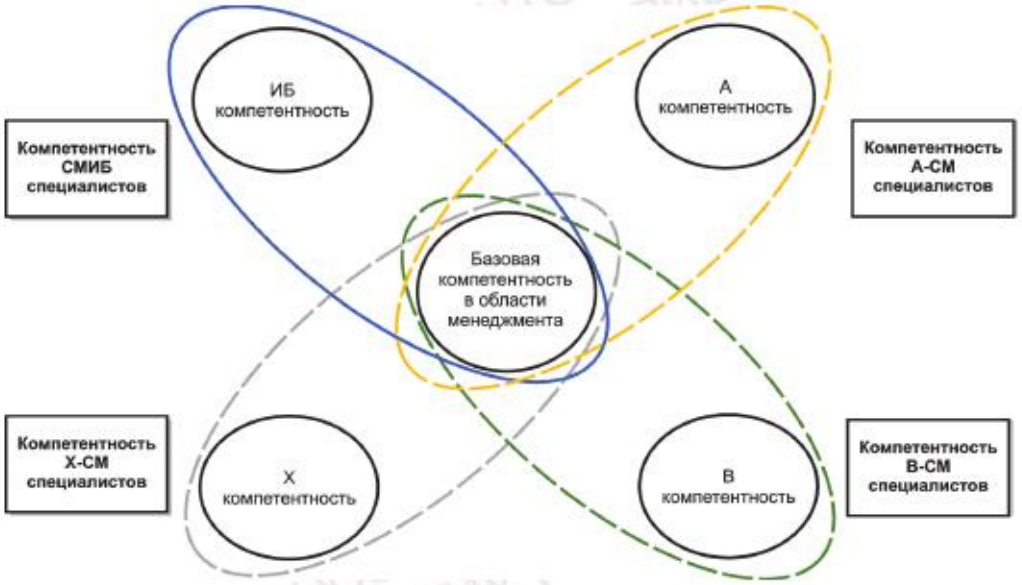

Рисунок 1 — Связь профессиональных компетентностей СМИБ-специалистов с общепрофессиональными компетентностями в области менеджмента и профессиональными компетентностями определенной предметной области

4.3 Структура компетентности СМИБ

Каждой компетентности присваиваются уникальное имя и уникальный номер, а также определяются ее индикаторы (требования к уровню знаний и навыков). Если применимы положения

ИСО/МЭК 27001:2013, определенные в его разделах с 5 по 10, то устанавливается связь между разделом стандарта и соответствующей компетентностью. В общем случае с разделом или подразделом могут иметь связи несколько компетентностей. Описание компетентности выполнено по шаблону, приведенному в таблице 1.

Таблица 1 — Шаблон для описания компетентности

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Номер и название раздела/подраздела
Ожидаемый результат	Описание ожидаемого результата как результат проявления СМИБ-специалистом компетентности
Требуемые знания	Краткое изложение тем, концепций и принципов, которые должны знать СМИБ-специалисты
Требуемые навыки	Навыки, которые СМИБ-специалисты способны реализовать

4.4 Демонстрация компетентности

СМИБ-специалисты для каждой компетентности должны быть способны продемонстрировать следующее:

a) знания, подтвержденные наличием определенной квалификации, полученной в результате обучения или практической работы;

b) навыки или способности решать задачи менеджмента или технические задачи.

4.5 Структура настоящего стандарта

В настоящем стандарте представлены компетентности, которыми должны обладать СМИБ-специалисты, разделенные на две категории. Эти категории относятся к общепрофессиональным компетентностям в области менеджмента и к профессиональным компетентностям в области информационной безопасности. В каждой категории определены по 12 компетентностей с привязкой к соответствующим группам процессов СМИБ (планирование, обеспечение, поддержка, функционирование, оценивание исполнения и улучшение). В настоящий стандарт включены следующие разделы и подразделы:

- 5 Общепрофессиональные компетентности в области менеджмента бизнеса для СМИБ-специалистов;
- 6 Компетентности в области информационной безопасности:
- 6.1 СМИБ-компетентность: информационная безопасность;
- 6.2 СМИБ-компетентность: планирование информационной безопасности;
- 6.3 СМИБ-компетентность: функционирование информационной безопасности;
- 6.4 СМИБ-компетентность: поддержка информационной безопасности;
- 6.5 СМИБ-компетентность: оценка эффективности информационной безопасности;
- 6.6 СМИБ-компетентность: улучшение информационной безопасности.

Приложение А содержит совокупности элементов, которые могут быть использованы при формировании свода знаний (СЗ) в организации, которыми должны обладать СМИБ-специалисты. Когда организация создает такой СЗ, то можно ссылаться на приложение А как на источник данных об уровне знаний СМИБ-специалистов.

5 Общепрофессиональные компетентности в области менеджмента бизнеса для СМИБ-специалистов

5.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобрести и обладать знаниями по фундаментальным областям менеджмента бизнеса и быть в курсе последних событий.

5.2 Компетентность: руководство

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	5 Руководство
Ожидаемый результат	Направлять, мотивировать и поощрять сотрудников в организации к выполнению ролей в области информационной безопасности
Требуемые знания	Теории лидерства; методы переговоров
Требуемые навыки	Формировать и установить направления деятельности организации в области информационной безопасности; предоставлять рекомендации, определять цели и стимулировать успешное решение задач, связанных с информационной безопасностью на различных уровнях их исполнения; выполнять взятые на себя обязательства; распределить обязанности и полномочия на разных уровнях организации

5.3 Компетентность: взаимодействие

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.4 Взаимодействие
Ожидаемый результат	Предоставлять правильную информацию в краткой форме соответствующим сторонам и обеспечивать наиболее продуктивное взаимодействие с руководством организации в отношении информационной безопасности
Требуемые знания	Теория и методы общения; методы анализа заинтересованных сторон; методы взаимодействия
Требуемые навыки	Разрабатывать процессы и каналы взаимодействия, подходящие для организации при создании СМИБ; общаться на соответствующем языке и с помощью средств массовой информации с широким кругом партнеров; налаживать отношения с высшим руководством и с организаторами бизнеса организации; определять потребности во внутренних и внешних взаимодействиях по вопросам СМИБ

5.4 Компетентность: бизнес-стратегия и СМИБ

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	4.1 Понимание внутренних и внешних факторов деятельности организации
Ожидаемый результат	Понимать, как формулируется бизнес-стратегия и как стратегия информационной безопасности и СМИБ вписывается в общую бизнес-стратегию
Требуемые знания	Бизнес-стратегия и процесс формулирования стратегии; правовая и нормативная среда, в которой работает организация; как определяется стратегия, например, с помощью дерева стратегического согласования

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	4.1 Понимание внутренних и внешних факторов деятельности организации
Требуемые навыки	Понимать бизнес-стратегию и стратегию организации; установить цели информационной безопасности в контексте бизнеса и его стратегии; продемонстрировать стратегическое направление в отношении СМИБ, начиная от планирования и кончая улучшением, которое направлено на достижение общих целей в области информационной безопасности; распределять или содействовать в распределении ресурсов для достижения целей бизнеса и информационной безопасности

5.5 Компетентность: менеджмент создания организации, культуры, поведения и заинтересованных сторон

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	4.2 Понимание потребностей и ожиданий заинтересованных сторон
Ожидаемый результат	Обеспечить соответствие внедрения СМИБ организационной структуре и культуре
Требуемые знания	Теория создания организации; теория организационной культуры; подходы, методологии и рамки организационного поведения; менеджмент конфликтов
Требуемые навыки	Понять структуру организации; понять тактику поведения организации; анализировать и оценивать культуру организации; интегрировать СМИБ в структуру организации; управлять участниками конфликта с разными интересами и вести переговоры для достижения целей безопасности

5.6 Компетентность: менеджмент проектирования процессов и изменений организации

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Поддерживать выполнение повседневных действий, связанных с информационной безопасностью
Требуемые знания	Оперативное планирование и контроль; методология и основы проектирования процессов; процессы документирования и процессы менеджмента записей; организационный контекст; методология и основы менеджмента изменений
Требуемые навыки	Руководить процессами и контролировать выполнение планов по достижению целей информационной безопасности; управлять процессами организации; управлять процессами аутсорсинга; управлять процессами менеджмента изменений; управлять записями

5.7 Компетентность: кадровый менеджмент, менеджмент коллективов и отдельных лиц

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.2 Квалификация
Ожидаемый результат	Активно действовать и разрабатывать организационные процессы для удовлетворения потребностей в развитии отдельных лиц, команд и всего персонала
Требуемые знания	Системы и процессы оценивания; методы совершенствования; методологии анализа квалификационных потребностей; методы образования и методы поддержки и развития (например, инструктаж, обучение, тренинг); оптимальные требования к персоналу и его квалификации, необходимые для внедрения и поддержки СМИБ; квалификации и сертификация, относящиеся к информационной безопасности
Требуемые навыки	Установить организационные и индивидуальные цели, задачи и задания и связать их; понимать и использовать такие стратегии, как расширение прав и возможностей; измерять и влиять на уровень мотивации сотрудников; использовать такие инструменты, как менеджмент производительности, постановка целей и оценки; инструктировать, и/или тренировать, и/или наставлять отдельных лиц или команды; работать в межфункциональных командах для достижения бизнес-целей и/или целей информационной безопасности; создавать культуру командной работы; поддерживать спецификации, собеседования, наем, отбор, обучение, надзор и развитие персонала с соответствующими навыками, опытом и мотивацией; оценивать результаты обучения, инструктажа и связанных с ними действий, а также приобретения навыков

5.8 Компетентность: менеджмент рисков

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Понимать методологию, основы и результаты менеджмента риска
Требуемые знания	Основные принципы риска; методология и основы менеджмента бизнес-риска, оценки и обработки рисков; правовая и нормативная база, с которой работает организация
Требуемые навыки	Понять определение риска и его компонентов в реальных условиях; понять методологию менеджмента бизнес-риска, методологию и процессы оценки и обработки риска; объяснять результаты менеджмента бизнес-риска или корпоративного риска

5.9 Компетентность: менеджмент ресурсов

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.1 Ресурсы
Ожидаемый результат	Обеспечить своевременное определение и предоставление соответствующих ресурсов для создания, внедрения, поддержки и постоянного улучшения СМИБ

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.1 Ресурсы
Требуемые знания	Финансовая отчетность и ее оценивание; методы создания и менеджмента бюджета; методы менеджмента затрат и методы их снижения; методы менеджмента времени и материалов; особенности анализа со стороны руководства и процессы корректирующих действий
Требуемые навыки	Определять ресурсы, необходимые для создания, внедрения, поддержки и постоянного улучшения СМИБ; бюджетировать бизнес-элементы, включая стоимость внедрения и стоимость эксплуатации СМИБ; понять финансовую отчетность, в том числе о движении денежных средств, прибылях и убытках; создавать бизнес-кейсы и инвестиционные кейсы; обеспечивать ROI (возврат инвестиций) и ROSI (возврат инвестиций в информационную безопасность) и другие финансовые преимущества; применять методы контроля затрат при менеджменте бюджета; своевременно предоставлять соответствующие ресурсы в нужном месте

5.10 Компетентность: архитектура информационных систем

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Понимать архитектуры применяемых информационных систем, используемых для создания, хранения, обработки, передачи и удаления информации организации
Требуемые знания	Требования к архитектуре информационных систем; аппаратные компоненты, инструменты и аппаратные архитектуры; операционные системы и программные платформы; интеграция бизнес-процессов и зависимость от бизнес-процессов приложений ИКТ; аспекты информационной безопасности архитектуры информационных систем
Требуемые навыки	Понять бизнес-цепи/драйверы, которые влияют на архитектуру информационной системы; понять взаимодействие компонентов безопасности и компонентов архитектуры информационной системы

5.11 Компетентность: менеджмент проектов и портфеля проектов

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Эффективно и действенно управлять различными типами проектов и действий, связанных со СМИБ (такими, как корректирующие, превентивные, улучшающие), для достижения намеченных результатов в нужное время, в рамках бюджета и требуемого качества

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Требуемые знания	Методологии и основы менеджмента проектов; методологии и основы менеджмента портфеля проектов; подходы к определению этапов проекта и инструменты для создания планов действий
Требуемые навыки	Управлять проектами, портфелем проектов, мероприятиями и задачами; управлять вместе с бизнесом портфелем инвестиционных проектов, связанных с СМИБ; планировать проекты для реализации стратегий, устанавливать процедуры и реализовывать их успешно и эффективно; работать в междисциплинарных группах для достижения целей бизнеса и/или информационной безопасности

5.12 Компетентность: менеджмент поставщиков

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Понимать роли поставщиков и цепочек поставок в организацию и их влияние на информационную безопасность
Требуемые знания	Методы использования поставщиков и цепочек поставок
Требуемые навыки	Оценить поставщиков и цепочку (и) поставок; оценить влияние на информационную безопасность поставщиков и цепочек поставок; управлять поставщиками при необходимости; предоставлять рекомендации по информационной безопасности при создании, оценке, выборе, менеджменте и завершении отношений с поставщиками

5.13 Компетентность: менеджмент проблем

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Своевременно выявлять и решать проблемы, которые могут иметь последствия для СМИБ
Требуемые знания	Методология и основы решения проблем и анализа
Требуемые навыки	Понять внутренние и внешние проблемы; анализировать и обобщать информацию и данные о проблемах; аналитически описывать проблемы менеджмента, применения аналитических подходов и разработки решений проблем; представлять и объяснять предлагаемые решения соответствующей аудитории

6 Компетентности в области информационной безопасности для СМИБ-специалистов

6.1 СМИБ-компетентность: информационная безопасность

6.1.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобретать и поддерживать в актуальном состоянии основную информацию о методах, средствах

и процессах информационной безопасности, являющуюся общей для управления информационной безопасностью, проектирования и эксплуатации, такую как ключевые принципы и цели информационной безопасности.

6.1.2 Компетентность: руководство деятельностью по обеспечению информационной безопасности

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Обеспечивать поддержку, направленную на высокий уровень СМИБ
Требуемые знания	Основы делового и/или корпоративного руководства; концепции и основы руководства деятельностью по обеспечению информационной безопасности; стандарты руководства деятельностью по обеспечению информационной безопасности (например, ИСО/МЭК 27014); правовые и нормативные вопросы, связанные с СМИБ; руководство деятельностью по менеджменту предприятия и менеджменту ИТ, а также соответствующие международные стандарты
Требуемые навыки	Разрабатывать структуру руководящих действий, которая соответствует/поддерживает структуру руководящих действий по менеджменту бизнеса; определять требования к отчетности и контролю; создавать, внедрить и поддерживать структуру руководящих действий по обеспечению информационной безопасности; излагать принципы руководства деятельностью по обеспечению информационной безопасности; обеспечивать информационную безопасность всей организации; принимать подход, основанный на оценке риска; задавать направление инвестиционных решений; обеспечивать соответствие внутренним и внешним решениям; создавать благоприятную для безопасности среду; понимать и определять объем правовых, нормативных и руководящих требований, которые могут повлиять на СМИБ; определять роли и обязанности в определенной области

6.1.3 Компетентность: контекст организации

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	4.1 Понимание внутренних и внешних факторов деятельности организации 4.2 Понимание потребностей и ожиданий заинтересованных сторон
Ожидаемый результат	Выявлять внутренние и внешние проблемы, которые могут повлиять на СМИБ
Требуемые знания	Методология и основы анализа контекста организации; организационная культура; схема информационных потоков; контекст организации, в которой будет внедрена СМИБ; правовая/нормативная база, касающая СМИБ
Требуемые навыки	Определять заинтересованные стороны, связанные с СМИБ, и выявлять требования этих заинтересованных сторон; определять области действия СМИБ, границы применимости СМИБ и заинтересованных лиц; сообщать заинтересованным сторонам о целях и преимуществах СМИБ; определять предполагаемый результат(ы) СМИБ

6.2 СМИБ-компетентность: планирование информационной безопасности

6.2.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобретать и постоянно обновлять информацию о планировании СМИБ.

6.2.2 Компетентность: область действия СМИБ

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	4.3 Определение области действия системы менеджмента информационной безопасности 6.2 Цели информационной безопасности и планы по их достижению
Ожидаемый результат	Продемонстрировать стратегическое направление в отношении СМИБ, начиная от планирования и заканчивая улучшением, которое направлено на достижение общей цели в области информационной безопасности
Требуемые знания	Цели информационной безопасности и планирования их достижения; области руководства деятельностью по обеспечению информационной безопасности; области политики информационной безопасности
Требуемые навыки	Разрабатывать, поддерживать и распространять стратегии и политики информационной безопасности в соответствии с бизнес-стратегией; определять заинтересованные стороны и их требования; руководить стратегическим планированием информационной безопасности для СМИБ; объяснять преимущества внедрения СМИБ для бизнеса; создавать СМИБ организации, соответствующую стратегии организации; понимать вопросы, относящиеся к целям организации и СМИБ; понимать и определять область действия СМИБ; синтезировать потребности, ожидания и требования для определения движущих сил СМИБ; определять организационные роли, обязанности в отношении СМИБ; понимать и генерировать ключевые показатели эффективности, ключевые показатели риска и другие бизнес-показатели для стратегий информационной безопасности и СМИБ

6.2.3 Компетентность: оценка и обработка рисков информационной безопасности

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	6.1 Действия по рассмотрению рисков и возможностей 8.2 Оценка рисков информационной безопасности 8.3 Обработка рисков информационной безопасности
Ожидаемый результат	Применять общие методы менеджмента риска (см. 5.8 Компетентность: менеджмент риска) к рискам информационной безопасности
Требуемые знания	Методология и области оценки/обработки рисков информационной безопасности; оценка рисков информационной безопасности; обработка рисков информационной безопасности; стандарты, относящиеся к рискам и рискам информационной безопасности (например, ИСО 31000 и ИСО/МЭК 27005; меры и средства информационной безопасности и цели их применения, как это указано в ИСО/МЭК 27001:2013, приложение А
Требуемые навыки	Предоставлять указания и рекомендации по оцениванию рисков информационной безопасности и контролировать соблюдение стандартов информационной безопасности и соответствующих политик информационной безопасности; определять и адресовать бизнес-риски, определять возможности, интегрированность и внедрение действий в процессы СМИБ; определять и применять процессы оценки и обработки рисков информационной безопасности; выбирать, внедрять и улучшать средства контроля для снижения риска информационной безопасности; сравнивать применяемые средства с теми, которые указаны в ИСО/МЭК 27001:2013, приложение А, и убедиться, что не были пропущены необходимые средства

6.3 СМИБ-компетентность: функционирование информационной безопасности

6.3.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобретать и постоянно обновлять информацию о работе и функционировании СМИБ.

6.3.2 Компетентность: функционирование информационной безопасности

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	8 Функционирование
Ожидаемый результат	Эффективно и действенно выполнять процессы, связанные с информационной безопасностью
Требуемые знания	Методология и основы менеджмента активов; методология и основы контроля доступа; методология и основы проектирования информационной безопасности; методология и основы физической защиты и защиты окружающей среды; методология и основы безопасности связи; методология и основы приобретения, разработки и сопровождения систем; методология и основы менеджмента инцидентов информационной безопасности; методология и основы аварийного восстановления; методология и основы обеспечения непрерывности бизнеса; методология и основы оценки соответствия; методология и основы менеджмента изменений и конфигураций; оценка и обработка рисков информационной безопасности; информационные технологии; жизненный цикл программного обеспечения и основы методологии; основы работы и внедрение широко распространенных средств менеджмента информационной безопасности; меры и средства менеджмента информационной безопасности, как указано в ИСО/МЭК 27001:2013, приложение А
Требуемые навыки	Управлять информационной безопасностью в процессах, переданных на аутсорсинг; выполнять процессы оценки рисков информационной безопасности; внедрять план обработки рисков информационной безопасности; оценивать уровни процессов и уровни функционирования, отнесенные к информационной безопасности; оценивать уровень информационной безопасности в других бизнес-процессах / операциях в организации

6.4 СМИБ-компетентность: поддержка информационной безопасности

6.4.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобретать и постоянно обновлять информацию о поддержке СМИБ.

6.4.2 Компетентность: осведомленность об информационной безопасности, образование и обучение

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.3 Осведомленность
Ожидаемый результат	Распространять культуру информационной безопасности среди персонала, работающего в рамках СМИБ

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	7.3 Осведомленность
Требуемые знания	Информация об информационной безопасности, образовании, подходах к подготовке и ее методах; подходы и стили обучения; педагогические подходы и методы обучения; методики анализа потребностей в обучении
Требуемые навыки	Создавать программы обучения и повышения осведомленности и консультировать операционные подразделения на всех уровнях по политике информационной безопасности, их вкладу в эффективность СМИБ, передовой практике; поддерживать осведомленность о состоянии безопасности защищенных информационных систем; определять требования к осведомленности, обучению и образованию; создавать информационные, образовательные и обучающие сообщения в области информационной безопасности и распространять их среди различных аудиторий; оценить и предложить механизмы соблюдения и поддержки культуры информационной безопасности

6.4.3 Компетентность: документирование

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	6.2 Цели информационной безопасности и планы по их достижению 7.5 Документированная информация
Ожидаемый результат	Управлять жизненным циклом документации по менеджменту информационной безопасности
Требуемые знания	Документация, требуемая для СМИБ; инструменты для разработки, редактирования и распространения документированной информации; инструменты и методы менеджмента версий документации; системы менеджмента документации
Требуемые навыки	Определять и предоставлять информацию, которая должна быть задокументирована для СМИБ; создавать и изменять описи документации для СМИБ; управлять изменениями документов и контролировать их версии; управлять шаблонами общих публикаций; организовывать и контролировать рабочие процессы менеджмента документации; документировать и каталогизировать основные процессы и процедуры

6.5 СМИБ-компетентность: оценка эффективности информационной безопасности

6.5.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны приобретать и постоянно обновлять информацию об оценке эффективности СМИБ.

6.5.2 Компетентность: мониторинг, оценка защищенности, анализ и оценивание СМИБ

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	9.1 Мониторинг, оценка защищенности, анализ и оценивание
Ожидаемый результат	Оценивать показатели информационной безопасности и эффективности СМИБ для поддержки организационных решений по постоянному улучшению СМИБ

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	9.1 Мониторинг, оценка защищенности, анализ и оценивание
Требуемые знания	Характеристики мониторинга и оценки защищенности; методы сбора и представление количественных и качественных данных; тенденции в менеджменте информационной безопасности и бизнес-среде
Требуемые навыки	Осуществлять мониторинг, проводить оценку защищенности и оценивать, реализуются ли процессы в соответствии с политиками информационной безопасности; устанавливать критерии и процессы оценки для: – внедрения СМИБ; – развертывания ресурсов менеджмента, организационной структуры и СМИБ; – количественной оценки инцидентов информационной безопасности; – соблюдения законов и правил; оценивать эффективность СМИБ; оценивать по следующим пунктам: если СМИБ была внедрена точно; внедрение менеджмента, организационной структуры и ресурсов СМИБ было надлежащим; количество инцидентов информационной безопасности было уменьшено; нарушения законов и правил не произошло; анализировать все системно ориентированные планы информационной безопасности во всей сети организации, действуя в качестве связующего звена с информационными системами; анализировать предлагаемые исключения из политик информационной безопасности; анализировать причины и извлекать уроки из фактов недостижения целей информационной безопасности

6.5.3 Компетентность: аудит СМИБ

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	9.2 Внутренний аудит
Ожидаемый результат	Периодически оценивать уровень соответствия СМИБ внешним и внутренним правилам
Требуемые знания	Методология и основы аудита информационной безопасности; процессы и процедуры внутреннего и внешнего аудита; роль и функции аудита, как внутреннего, так и внешнего; методы оценки, тестирования и выборочного исследования информационной безопасности
Требуемые навыки	Управлять внутренними аудитами СМИБ; установить или повлиять на объем аудита информационной безопасности; анализировать результаты одного или нескольких аудитов информационной безопасности; предлагать инициативы, мероприятия, проекты и программы с соответствующими требованиями к ресурсам для рассмотрения выводов, рекомендаций и пунктов аудита; готовить отчет о соблюдении обязательств; наблюдать, руководить, управлять и участвовать в аудитах информационной безопасности; описывать, руководить и обеспечивать планы и процессы тестирования информационной безопасности и аудиторские отчеты; анализировать тенденции применительно к менеджменту информационной безопасности, к результатам аудита СМИБ и бизнес-среде; отслеживать признаки инцидентов информационной безопасности до соответствующих элементов СМИБ

6.5.4 Компетентность: проверка со стороны руководства

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	9.3 Проверка со стороны руководства 10.1 Несоответствие и корректирующие действия
Ожидаемый результат	Обеспечивать постоянное улучшение, адекватность и эффективность СМИБ
Требуемые знания	Методы менеджмента риска; финансовая отчетность и ее оценка; методы менеджмента бюджета; менеджмент затрат и методы их снижения
Требуемые навыки	Определять подходящий интервал для страхования эффективности СМИБ; провести анализ целей СМИБ, бюджеты, бизнес-показатели и подтвердить соответствующие действия; сообщать результаты анализа со стороны руководства заинтересованным сторонам, если это необходимо; влиять на результативность и эффективность информационной безопасности на основе результатов анализа со стороны руководства; успешно председательствовать на собрании по обсуждению результативности менеджмента

6.6 СМИБ-компетентность: улучшение информационной безопасности

6.6.1 Общие сведения

Для успешного и эффективного выполнения своих ролей в организации СМИБ-специалисты должны формировать и постоянно поддерживать в актуальном состоянии свой потенциал в отношении улучшения СМИБ.

6.6.2 Компетентность: постоянное улучшение

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	10.2 Постоянное улучшение
Ожидаемый результат	Включаться в процесс, направленный на постоянное улучшение своевременным образом всех ключевых аспектов СМИБ
Требуемые знания	Методология и основы постоянного улучшения
Требуемые навыки	Решать, следует ли поддерживать текущую СМИБ; эффективно выполнять корректирующие действия; определять, как применение процесса постоянного улучшения будет поддерживать цели СМИБ; предлагать корректирующие действия; учитывать новые законодательные и нормативные требования и обязательства; предлагать механизмы для улучшения приемлемости, адекватности и результативности СМИБ

6.6.3 Компетентность: технологические тенденции и развитие

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Ожидаемый результат	Согласовывать существующую СМИБ с последними технологическими инновациями с особым вниманием к рискам информационной безопасности, которые они могут снизить или создать
Требуемые знания	Новые технологии и их применение

Окончание таблицы

ИСО/МЭК 27001:2013 раздел/подраздел (если применимо)	Разделов или подразделов стандарта, которые можно применить, нет
Требуемые навыки	Создавать картину будущих технологий, угроз и рисков и изменять текущую СМИБ, чтобы обеспечить ее постоянную приемлемость, адекватность и результативность; анализировать влияние на бизнес новых технологий, таких как искусственный интеллект

Приложение А
(справочное)

Совокупность терминов, характеризующих необходимые знания для СМИБ-специалистов как часть свода знаний

В этом приложении представлены элементы, которые можно использовать при формировании свода знаний (СЗ) в организации. Организации может потребоваться больше таких элементов, чем приведено в данном приложении, и она может создать свой свод знаний, специфичный для этой организации.

Свод знаний должен содержать полный набор концепций, терминов и действий, составляющих профессиональную область СМИБ, как это определено соответствующим научным обществом или профессиональной ассоциацией. Ниже приведенная таблица А.1 является иллюстративной и содержит примеры терминов, характеризующие необходимые знания в отношении определенным компетентностям, которые могут быть использованы для создания СЗ.

Таблица А.1 — Примеры терминов, характеризующих необходимые знания, относящиеся к компетентностям СМИБ-специалистов, которые могут быть использованы для создания СЗ

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
5 Бизнес-компетентности	5.2 Руководство	Приверженность, постоянное улучшение, требования СМИБ, вдохновение, мотивация, влияние, переговоры, организационный авторитет, ответственность, организационная роль, цель организации, стратегическое направление, высшее руководство
	5.3 Взаимодействие	Внутренняя и внешняя проблема, презентация, менеджмент взаимодействия, план взаимодействия, безопасность взаимодействия, культура заинтересованных сторон, менеджмент документации, целевая аудитория, внутреннее и внешнее взаимодействие, сотрудник по связям с общественностью, менеджмент заинтересованных сторон, заинтересованная сторона, анализ заинтересованных сторон, высшее руководство
	5.4 Бизнес-стратегия и СМИБ	Бизнес-метрики (сбалансированная система показателей (BSC), показатели ключевых целей (KGI), ключевые показатели эффективности (KPI), бизнес-стратегия, правовая и нормативная база
	5.5 Менеджмент создания организации, культуры, поведения и заинтересованных сторон	Анализ/оценка поведения, контроль мотивации, полномочия, организация, организационный дизайн (создание организации), организационная культура, анализ заинтересованных сторон
	5.6 Менеджмент проектирования процессов и изменений организации	Антивирусное программное обеспечение, базовый уровень, менеджмент конфигураций, контроль, цель контроля, коррекция, менеджмент идентификации, менеджмент рисков информационной безопасности, оценка рисков, обработка рисков информационной безопасности, библиотека инфраструктур информационной технологии (ITIL), внутренняя угроза, цель, процесс, модель зрелости процессов, риск, анализ данных безопасности, менеджмент событий информационной безопасности (SIEM), меры безопасности, системный журнал, система мониторинга, анализ угроз, мониторинг угроз, анализ уязвимостей

Продолжение таблицы А.1

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
5 Бизнес-компетентности	5.7 Менеджмент человеческих ресурсов, коллективов и отдельных лиц	Траектория обучения, контроль мотивации, расширение прав и возможностей, аттестации базовой квалификации, сертификация, компетентность, компьютерное обучение (CBT), соответствие, дисциплинарный процесс, обучение и образование конечных пользователей, занятость человеческих ресурсов, подготовка кадров и образование, осведомленность об информационной безопасности, учебная программа по информационной безопасности, трудовое пиратство, ответственность руководства, квалификация, ролевое обучение, отбор, веб-обучение (WBT)
	5.8 Менеджмент рисков	Атака, анализ воздействия на бизнес, бизнес-риски, общение и консультация, последствия, постоянное улучшение, контроль, событие, событие информационной безопасности, уровень риска, вероятность, мониторинг, остаточный риск, обзор, риск, принятие риска, анализ риска, оценка риска, отношение к риску, риск-аппетит, толерантность к риску, информирование о рисках и консультации, критерии рисков, оценка рисков, идентификация рисков, менеджмент риска, основы менеджмента риска, процесс менеджмента риска, владелец риска, профиль риска, источник риска, обработка риска, заинтересованная сторона, угроза, уязвимость
	5.9 Менеджмент ресурсов	Бизнес-метрики (BSC, KGI, KPI), анализ, менеджмент бюджета, составление бюджета СМИБ, стоимость, затраты и выгоды от внедрения СМИБ, расходы, финансовые принципы, менеджмент финансов, финансовый отчет, чистая приведенная стоимость (NPV), внутренняя норма прибыли (IRR), инвестиции, оценка инвестиций, рентабельность инвестиций (ROI), ключевой показатель эффективности, административная дисциплина, рентабельность инвестиций в безопасность (ROSI), KPI безопасности
	5.10 Архитектура информационных систем	Менеджмент конфигураций, данные, информационная потребность, требование информационной безопасности (анализ и спецификация), доступность, менеджмент изменений, облачный сервис, система баз данных, документация, средства обработки информации, архитектура информационной безопасности, инцидент информационной безопасности, информационная система, отказ информационной системы, архитектура информационной системы, ремонтопригодность, договор на обслуживание, стоимость обслуживания, сетевая архитектура, аутсорсинговая разработка, менеджмент исправлений, повторная разработка/обновление, надежность, требования, спецификация безопасности, анализ уязвимостей безопасности, безопасное кодирование, принципы безопасного кодирования, безопасная среда разработки, политика безопасной разработки, безопасное проектирование системы, принципы проектирования безопасных систем, обеспечение программного обеспечения, стабильность, приемочное тестирование системы, жизненный цикл развития системы (SDLC), менеджмент проектов разработки системы, системная инженерия, тестирование безопасности системы, удобство использования
	5.11 Менеджмент проектов и портфеля проектов	Контроль, заинтересованное лицо, деятельность, утверждение и расстановка приоритетов, исходный уровень, запрос на изменение, менеджмент конфигураций, корректирующее действие, критический путь, групповая динамика, проект СМИБ, отставание, траектория обучения, жизненный цикл проекта, менеджер проекта, реестр рисков, тендер, иерархическая структура работ (WBS)

Продолжение таблицы А.1

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
5 Бизнес-компетентности	5.12 Менеджмент поставщиков	Требование информационной безопасности (анализ и спецификация), заинтересованное лицо, анализ воздействия на бизнес, анализ рисков, менеджмент контрактов, анализ затрат и выгод, утилизация, криминалистическая экспертиза информационной безопасности (форензика), политика информационной безопасности, заинтересованная сторона, законы и постановления, аутсорсинг, предварительная оценка, соответствие нормативным требованиям, запрос предложений (RFP), снижение рисков, риск — обоснованное решение, соглашение об уровне обслуживания (SLA), ходатайство, заявление о целях (SOO), техническое задание (SOW), общая стоимость владения (TCO)
	5.13 Менеджмент проблем	Анализ и синтез, аналитическая модель, аналитическое мышление, оценка, когнитивная наука, критический фактор успеха (CSF), критическое мышление, данные, критерии принятия решения, производная мера, оценка, индикатор, потребность информационная, требование информационной безопасности (анализ и спецификация), внутренняя и внешняя проблема, измерение, презентация, подход к решению проблем, методологии решения проблем, масштаб, проверка (валидация)
6 СМИБ-компетентности		
6.1 Информационная безопасность	6.1.2 Руководящая деятельность по обеспечению информационной безопасности	Заинтересованное лицо, судебная экспертиза информационной безопасности (форензика), заинтересованная сторона, руководство деятельностью по менеджменту, руководящая деятельность по обеспечению информационной безопасности, руководящий орган, область руководящей деятельности по обеспечению информационной безопасности, риск информационной безопасности, внутренний контекст, цели и задачи организации, программный ресурс
	6.1.3 Контекст организации	Приверженность, постоянное улучшение, требования СМИБ, лидерство, переговоры, авторитет организации, ответственность организации, роль организации, цель организации, стратегическое направление, высшее руководство
6.2 Планирование информационной безопасности	6.2.2 Область действия СМИБ	(Информационный) актив, базовая мера, бизнес-преимущества СМИБ, менеджмент, цель менеджмента, исправление, затраты и выгоды от внедрения СМИБ, критический фактор успеха (CSF), эффективность, исполнительное руководство, внешний контекст, информационная безопасность, средства менеджмента информационной безопасности, меры обеспечения информационной безопасности, политика информационной безопасности, роль и ответственность информационной безопасности, проект СМИБ, ключевой показатель эффективности, правоохранительный орган, система менеджмента, политика мобильных устройств, новая платформа, неотказуемость, объект, цель, организация, политика, превентивные действия, надежность, рентабельность инвестиций в безопасность (ROSI), анализ политик информационной безопасности, риск, критерии принятия риска, менеджмент риска, процесс менеджмента рисков, разделение обязанностей, группы особых интересов, удаленная работа, высшее руководство

Продолжение таблицы А.1

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
6.2 Планирование информационной безопасности	6.2.3 Оценка и воздействие на риски информационной безопасности	Приемлемый риск, ожидаемая годовая потеря, годовая частота возникновения, атака, доступность, стратегия резервного копирования, базовый уровень, базовое моделирование, бенчмаркинг, непрерывность бизнеса, анализ влияния бизнеса, бизнес-метрики (BSC, KGI, KPI), план восстановления бизнеса, управление изменениями, конфиденциальность, делегирование полномочий, цифровая идентификация, аварийное восстановление, событие, развитие человеческих ресурсов, средства обработки информации, очистка ИБ, непрерывность ИБ, событие ИБ, инцидент ИБ, оценка риска ИБ, управление рисками ИБ, обработка рисков ИБ, план чрезвычайных ситуаций информационной системы, инсайдерская угроза, взаимодействующие коммуникации, ротация должностей, лидерство, уровень риска, вероятность, управленческие возможности, минимальная цель непрерывности бизнеса (MBCO), обеспечение миссии, мониторинг, соглашение о неразглашении, аварийный план, порядок преемственности, чувствительность позиции, предварительная подготовка / готовность, превентивные действия, цель точки восстановления (RPO), цель времени восстановления (RTO), остаточный риск, принятие риска, критерии принятия риска, анализ риска, оценка риска, критерии оценки риска, идентификация риска, уровень риска, процесс управления риском, смягчение риска, владелец риска, источник риска, обработка рисков, нарушение безопасности, стандарт реализации безопасности, реагирование на инциденты безопасности, разделение обязанностей, социальная инженерия, специальное фоновое расследование (BOO), заинтересованная сторона, риск информационной безопасности, законы и нормативные акты, доступность, средства обработки информации, требование, внутренняя и внешняя проблема, организация, атака, конфиденциальность, оценка риска ИБ, управление рисками ИБ, обработка рисков ИБ, целостность, цель, планирование (процесс СМИБ)
6.3 Функционирование информационной безопасности	6.3.2 Функционирование информационной безопасности	(Информационный) актив, контроль доступа, аккредитация, антивирусное программное обеспечение, менеджмент активов, аутентификация, доступность, резервное копирование, базовый уровень безопасности, определение причины, менеджмент изменений, безопасность связи, группа реагирования на инциденты компьютерной безопасности (CSIRT), конфиденциальность, менеджмент конфигураций, криптография, аварийное восстановление, документация, экологическая безопасность, менеджмент идентификаций, обработка инцидентов, группа реагирования на инциденты, архитектура ИБ, инженерия ИБ, криминалистика информационной безопасности, инцидент информационной безопасности, менеджмент инцидентов информационной безопасности, оценка системы информационной безопасности, библиотека инфраструктуры информационных технологий (ITIL), инсайдерские угрозы, интегрированная среда разработки, ремонтопригодность, стоимость обслуживания, менеджмент исправлений, тестирование на проникновение, физическая безопасность, профилактическое обслуживание, метод проверки, информирование о рисках и консультации, риск снижения последствий, анализ данных безопасности, тестирование оценки безопасности, меры безопасности, анализ требований безопасности, спецификация безопасности, тестирование и оценка безопасности, анализ уязвимостей безопасности, принципы безопасного кодирования, методы безопасного программирования, безопасное проектирование

Продолжение таблицы А.1

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
6.3 Функционирование информационной безопасности	6.3.2 Функционирование информационной безопасности	системы, обеспечение безопасности программного обеспечения, стабильность, приобретение системы, жизненный цикл разработки системы (SDLC), менеджмент проектов разработки системы, системная инженерия, повышение защищенности системы, системный журнал, мониторинг системы, средства технического контроля безопасности, инструменты тестирования, анализ угроз, удобство использования
6.4 Поддержка информационной безопасности	6.4.2 Осведомленность об информационной безопасности, образование и обучение	Базовый уровень, компьютерное обучение (CBT), учебный план, документация, обучение и образование конечных пользователей по вопросам безопасности, обучение персонала и образование, осведомленность об информационной безопасности, учебная программа по информационной безопасности, траектория обучения, система менеджмента обучения (LMS), цели обучения, оценка потребностей, ролевое обучение, тест, тестирование, веб-обучение (WBT)
	6.4.3 Документирование	Архивирование, менеджмент изменений, классификация, уничтожение, утилизация, критерии документации, менеджмент документации, методологии документирования, технологии документирования, документированная информация, метаданные, онтология, менеджмент записей, менеджмент версий
6.5 Оценка эффективности информационной безопасности	6.5.2 Мониторинг, оценка защищенности, анализ и оценивание СМИБ	Подотчетность, анализ и синтез, оценка, аудит, кодекс этики, менеджмент контрактов, контроль, производная мера, оценивание, руководящая деятельность, руководящие принципы, судебная экспертиза информационной безопасности, показатели информационной безопасности, политика информационной безопасности, законы и правила, мера, измерение, функция измерения, метод измерения, результат измерения, мониторинг несоответствий, производительность, принципы конфиденциальности/честное (справедливое) использование информации, процедура, обзор, объект обзора, обзор действующих стандартов (международные/национальные/отраслевые стандарты, руководства и т. д.), доверенный объект передачи информации, единица измерения, валидация (аттестация), верификация
	6.5.3 Аудит СМИБ	Аудит, объект аудита, заключение аудита, критерии аудита, свидетельства аудита, выводы аудита, метод аудита, цель аудита, план аудита, программа аудита, область аудита, группа аудита, проверяемая организация, аудитор, аутентификация, соответствие, затраты и преимущества внедрения СМИБ, руководство, внутренний и внешний аудит, процесс СМИБ, область действия и границы СМИБ , несоответствие, наблюдатель, принципы аудита, риск, объем аудита; аудиторские доказательства, технический эксперт

Продолжение таблицы А.1

Бизнес-компетентности (раздел 5), СМИБ-компетентности (раздел 6)	Компетентности	Примеры терминов, характеризующих необходимые знания
6.5 Оценка эффективности информационной безопасности	6.5.4 Проверка со стороны руководства	Менеджмент бюджета, бизнес-метрики (BSC, KGI, KPI), менеджмент коммуникаций, менеджмент затрат, финансы, менеджмент, цель, менеджмент рисков
6.6 Улучшение информационной безопасности	6.6.2 Постоянное улучшение	Одобрение и расстановка приоритетов, определение причины, постоянное улучшение, корректирующие действия, обеспечение непрерывности информационной безопасности, несоответствие
	6.6.3 Технологические тенденции и развитие	Критическая инфраструктура, цифровое правительство, сообщество обмена информацией, новая платформа, написание сценария, стандарт реализации обеспечения безопасности, социальное видение, методологии прогнозирования технологии

Приложение ДА
(справочное)

Сведения о соответствии ссылочного международного стандарта национальному стандарту

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

Библиография

[1] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

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

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

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

УДК 006.035:004.056.5:004.057.2:006.354 ОКС 35.040

Ключевые слова: безопасность, информационная безопасность, обеспечение безопасности, система, менеджмент, система менеджмента информационной безопасности, политика информационной безопасности, компетентность, знания, навыки, мера, средства, требования, эффективность

Редактор *Д.А. Кожемяк*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 21.05.2021. Подписано в печать 28.05.2021. 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