МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/IEC 19896-1— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий

Часть 1

Введение, основные понятия и общие требования

(ISO/IEC 19896-1:2018, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Центр безопасности информации» и Обществом с ограниченной ответственностью «Информационно-аналитический центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Федеральным агентством по техническому регулированию и метрологии

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 июня 2021 г. № 141-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 2 июля 2021 г. № 614-ст межгосударственный стандарт ГОСТ ISO/IEC 19896-1—2021 введен в действие в качестве национального стандарта Российской Федерации с 30 ноября 2021 г.

5 Настоящий стандарт идентичен международному стандарту ISO/IEC 19896-1:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий. Часть 1. Введение, основные понятия и общие требования» («Information technology — Security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements», IDT).

ISO/IEC 19896-1:2018 разработан подкомитетом SC 27 «Информационная безопасность, кибербезопасность и защита конфиденциальности» Совместного технического комитета JTC 1 «Информационные технологии» Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC).

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

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

6 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Содержание

Введение

Целью серии стандартов ISO/IEC 19896 является предоставление фундаментальных основ, относящихся к уровню подготовки лиц, ответственных за выполнение оценки безопасности продуктов ИТ[1)] и тестирование соответствия. Серия ISO/IEC 19896 описывает основы и специализированные требования, которые определяют минимальную компетенцию лиц, выполняющих оценку безопасности продуктов ИТ и тестирование соответствия с использованием установленных стандартов.

Для достижения этой цели серия стандартов ISO/IEC 19896 включает следующее:

a) термины и определения, относящиеся к тематике уровня компетенции специалистов по тестированию и оценке безопасности продуктов ИТ;

b) фундаментальные концепции, относящиеся к компетенции в оценке безопасности и тестировании соответствия продуктов ИТ;

c) минимальные требования к компетенции специалистов по оценке безопасности и тестированию продуктов ИТ для проведения тестирования/оценки продуктов ИТ.

Серия стандартов ISO/IEC 19896 представляет интерес:

a) для специалистов по оценке информационной безопасности (ИБ)[2)] и тестированию соответствия;

b) органов подтверждения соответствия по оценке ИБ технологий и тестированию соответствия;

c) лабораторий, занимающихся оценкой ИБ и проверкой соответствия требованиям;

d) производителей или поставщиков технологий, чьи продукты ИТ могут быть предметом оценки обеспечения ИБ или тестирования соответствия;

e) организаций, предоставляющих профессиональные полномочия или признание в области компетенции.

Серия стандартов ISO/IEC 19896 разделена на части, предназначенные для специалистов по тестированию и оценке, как указано далее.

В настоящем стандарте представлены обзор определений, основных понятий и общее описание основ, используемых для представления требований к знаниям для определенных специализированных областей. Настоящий стандарт нацелен на предоставление фундаментальных знаний, необходимых для использования общих основ, представленных в других соответствующих частях серии ISO/IEC 19896.

ISO/IEC 19896-2 описывает минимальный набор требований к компетенции на каждом уровне подготовки для специалистов по тестированию соответствия, работающих с ISO/IEC 19790 и соответствующими стандартами.

ISO/IEC 19896-3 описывает минимальный набор требований к компетенции на каждом уровне подготовки для специалистов по оценке соответствия требованиям по ИБ, работающих с ISO/IEC 15408 (все части) и соответствующими стандартами.

---

1) ИТ — информационные технологии (примечание переводчика).

2) Далее по тексту используется сокращение ИБ.

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Требования к компетенции специалистов по тестированию и оценке безопасности информационных технологий

Часть 1

Введение, основные понятия и общие требования

Information technology. Security techniques.
Competence requirements for information security testers and evaluators.
Part 1. Introduction, concepts and general requirements

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт определяет термины и устанавливает упорядоченный набор понятий и отношений для понимания требований к компетенции для специалистов по тестированию соответствия и оценке обеспечения ИБ, тем самым создавая основу для общего понимания концепций и принципов, лежащих в основе серии ISO/IEC 19896 для всех пользователей ее сообщества. Настоящий стандарт предоставляет основополагающую информацию для пользователей серии ISO/IEC 19896.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты [для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения)]:

ISO/IEC 17000, Conformity assessment — Vocabulary and general principles (Оценка соответствия. Словарь и общие принципы)

ISO/IEC 17025, General requirements for the competence of testing and calibration laboratories (Оценка соответствия. Общие требования к компетенции испытательных и калибровочных лабораторий)

3 Термины и определения

В настоящем стандарте применены термины по ISO/IEC 17000 и ISO/IEC 17025, а также следующие термины с соответствующими определениями:

ISO и IEC ведут терминологические базы данных для их использования в стандартизации по следующим адресам:

- платформа онлайн-просмотра ISO: доступна по адресу http://www.iso.org/obp;
- Электропедия IEC: доступна по адресу http://www.electropedia.org/;
- термины и определения ITU-T: http://www.itu.int/go/terminology-databasehttp://www.itu.int/go/terminology-databasehttp://www.itu.int/go/terminology-database

Издание официальное

3.1 **компетенция** (competence): Способность применять знания и навыки для достижения намеченных результатов.

[ISO/IEC 17024:2012, 3.6]

3.2 **специалист по тестированию соответствия, тестировщик** (conformance-tester, tester): Специалист, назначаемый для выполнения действий по тестированию в соответствии с применимым стандартом тестирования соответствия и соответствующей методологией испытаний.

Примечание — Примером такого стандарта является ISO/IEC 19790 и методология испытаний, приведенная в ISO/IEC 24759.

3.3 **образование** (education): Процесс получения или предоставления систематического обучения, преимущественно в школе или университете.

3.4 **эффективность** (effectiveness): Способность продуктивно применять знания и навыки, характеризующаяся такими признаками поведения, как предрасположенность, инициатива, энтузиазм, готовность, коммуникативные навыки, работа в команде и лидерство.

3.5 **оценщик** (evaluator): Лицо, назначенное для проведения оценки в соответствии с применимым стандартом оценки и соответствующей методологией оценки.

Примечание — Примером стандарта оценки является ISO/IEC 15408 (все части) с соответствующей методологией оценки, приведенной в ISO/IEC 18045.

3.6 **опыт** (experience): Участие на практическом уровне в проектах, относящихся к сфере компетенции.

3.7 **знание** (knowledge): Факты, сведения, информация, принципы или понимание, обретаемые с помощью опыта или образования.

Примечание — Примером знаний является способность описывать различные части стандарта по доверию к информации.

[ISO/IEC TS 17027:2014, 2.56, изменено — добавлено примечание 1]

3.8 **лаборатория** (laboratory): Организация с системой менеджмента, обеспечивающей проведение работ по оценке и/или тестированию в соответствии с определенным набором политик и процедур и использующая определенную методологию для тестирования или оценки функциональности безопасности продуктов ИТ.

Примечание — Этим организациям часто даются альтернативные названия различными регулирующими органами. Например, Центр оценки безопасности ИТ (IT Security Evaluation Facility, ITSEF), Лаборатория испытаний по общим критериям (Common Criteria Testing Laboratory, CCTL), Коммерческий центр оценки (Commercial Evaluation Facility, CLEF).

3.9 **навык** (skill): Способность выполнять задачу или работу с конкретным намеченным результатом, полученная в результате обучения, стажировки, опыта или другими методами.

Примечание — Примером навыков является способность идентифицировать и классифицировать риски, связанные с проектом.

[ISO/IEC 17027:2014, 2.74, изменено — добавлено примечание 1]

4 Концепции

Для обеспечения поддержки согласованности при оценке или тестировании соответствия продуктов безопасности ИТ одним из факторов является компетенция лиц, выполняющих работу по оценке или тестированию соответствия. Несмотря на предоставление стандартизированных методов оценки или тестирования соответствия, для поддержки достижения согласованности и повторяемости результатов требуется минимальная компетенция в выполнении необходимых действий. Это, в свою очередь, поддерживает взаимное признание сертификатов и подтверждений соответствия обеспечения безопасности продуктов ИТ.

ISO/IEC 17025 устанавливает общие требования к компетенции испытательных и калибровочных лабораторий и часто определяется как база для согласованности между лабораториями оценки и тестирования на соответствие требованиям по ИБ.

ISO/IEC 17025 определяет различные требования к компетенции лаборатории, которым она должна соответствовать. Они включают:

- обеспечение компетенции всего персонала, который может влиять на деятельность лаборатории;

- определение и документирование требований к компетенции для каждой функции, вовлеченной в деятельность лаборатории;

- обеспечение компетенции персонала лаборатории для выполнения той деятельности, за которую он несет ответственность; понимания важности и реагирования на отклонения, обнаруженные в отношении деятельности лаборатории;

- наличие документированного процесса постоянного мониторинга персонала, задействованного в работе лаборатории;

- ведение записей о компетенции, таких как образование, стажировка, технические знания, навыки, опыт, разрешения и мониторинг всего персонала, задействованного в работе лаборатории.

Примечание — ISO/IEC 17025 предназначен для широкого круга испытательных и калибровочных лабораторий и используется не только в области тестирования и оценки обеспечения безопасности продуктов ИТ.

5 Элементы компетенции

5.1 Компетенции

Для того, чтобы компетентно получить непротиворечивые результаты тестирования и оценки, обеспечить цель согласованности в результатах, предоставляемых различными специалистами и лабораториями, необходимо, чтобы специалисты по тестированию соответствия и оценке имели накопленный минимум необходимых знаний, навыков, опыта и квалификации, соответствующих целевому стандарту обеспечения безопасности продуктов ИТ, и были способны эффективно выполнять свои обязанности.

В данном разделе определены минимальные элементы компетенции, которые должны использоваться в стандартах серии ISO/IEC 19896 при рассмотрении требований к компетенции специалистов по тестированию соответствия и/или оценке для конкретных стандартов обеспечения безопасности продуктов ИТ.

Обучение может проводиться с целью повышения некоторых элементов компетенции сотрудников. Например, обучение часто проводится с целью приобретения или улучшения существующих навыков, повышения уровня знаний или для повышения эффективности.

Дополнительные элементы компетенции, такие как предрасположенность к чему-либо, энтузиазм, инициативность, лидерские качества, работа в команде и готовность, могут быть определены лабораториями или органами по аккредитации. Они также могут быть определены в других частях серии ISO/IEC 19896.

5.2 Знания

Обладание знаниями тестировщиками и оценщиками является одним из элементов компетенции. Ниже приведены сведения, формирующие основу для обеспечения подобающей и проверяемой совокупности знаний, связанной с настоящим стандартом обеспечения безопасности продуктов ИТ:

a) знание соответствующего стандарта обеспечения безопасности продуктов ИТ;

b) любые связанные методы тестирования или оценки;

c) политики и процедуры соответствующих регулирующих органов, органов по аккредитации и лабораторий;

d) знание архитектуры и проектов продуктов ИТ в соответствующих технологических областях.

При исследовании продуктов ИТ различные технологии могут иметь отношение к сфере работы лаборатории, и знание этих технологий следует учитывать при определении минимальных уровней компетенции. Для конкретной области технологий важны следующие категории знаний:

a) технологии, используемые при проектировании, разработке и внедрении испытываемых продуктов;

b) способ, которым продукты ИТ используются или предназначены для использования;

c) типичные уязвимости и опасные возможности, которые могут присутствовать в этой технологии;

d) область, в которой продукты ИТ используются или предназначены для использования.

Примеры технологических областей включают криптографию, биометрию, интегральные схемы, операционные системы, сетевые устройства, базы данных, смарт-карты и встроенные системы. Кроме того, технологические области иногда определяются регулирующим органом.

5.3 Навыки

Навыки, которые обычно требуются от специалистов по тестированию и оценке безопасности продуктов ИТ в соответствии с уровнями компетенции, определенными в разделе 6, включают:

a) понимание области применения и основ продукта оценки или тестирования соответствия;

b) понимание границ реализации для тестирования или цели оценки;

c) способность выбрать или адаптировать конкретный метод тестирования или оценки;

d) выполнение анализа документации;

e) понимание исходного кода, схем и базовых компонентов, используемых в определении и реализации продуктов;

f) разработку и выполнение функционального и нефункционального тестирования;

g) определение того, находятся ли условия испытаний в пределах установленных параметров, чтобы обеспечить повторяемость результатов испытаний;

h) калибровку и использование средств тестирования;

i) обеспечение надлежащего хранения, включая соответствующую целостность, доступность и конфиденциальность, данных тестирования, результатов испытаний и протоколов испытаний, включая разъяснения и отчеты об испытаниях;

j) интерпретацию результатов испытаний;

k) умение писать понятные отчеты с подробным описанием результатов своей работы;

l) способность повторить тест или воспроизвести заархивированный тест и получить те же результаты;

m) способность создать тестовую среду для достижения надлежащих условий работы безопасных продуктов.

На более высоких уровнях компетенции также могут быть востребованы такие навыки, как способность эффективного взаимодействия и управления проектами.

На уровнях компетенции 1 и 2 эти навыки могут применяться под наблюдением.

5.4 Опыт

Опытные специалисты — это специалисты, которые проводили оценки или тестирование соответствия и, возможно, учили или были наставниками других специалистов во многих проектах оценки или тестирования соответствия. У опытных специалистов есть глубокое понимание требований к проектам оценки или тестирования соответствия, а также каких-либо интерпретаций и политик органов по аккредитации, регулирующих органов и лабораторий.

5.5 Образование

Указание конкретной квалификации, например техник, бакалавр или более высокий уровень, может помочь определить способность специалиста следовать принятой программе или работать независимо.

Некоторые программы высшего образования и курсы, связанные с оценкой и тестированием соответствия, могут дать специалисту возможность получить профессиональные знания в области обеспечения ИБ.

В некоторых случаях может быть приемлемым заменить специалиста с профильным образованием или курсами на специалиста, обладающего соответствующим и релевантным опытом.

5.6 Эффективность

Эффективность специалиста по оценке или тестированию варьируется в зависимости от целей и структуры лаборатории так же, как и от целей и структуры регулирующего органа. В частности, требования к эффективности должны учитывать точность результатов тестирования или получаемых оценок, возможность повторения методов и мероприятий оценки или тестирования, выполняемых другими компетентными специалистами по тестированию и оценке, и получение тех же результатов, а также способность донести результаты тестирования и оценки таким образом, чтобы они были понятны целевой аудитории.

6 Уровни компетенции

6.1 Общие

Специалистам по оценке и тестированию может быть присвоен уровень компетенции для каждой конкретной области компетенции, приведенной в других частях серии ISO/IEC 19896. Они приведены в 6.2—6.5 в соответствии с номером уровня и содержат типовое описание.

Общие уровни компетенции могут использоваться для обозначения различного уровня владения профессиональными навыками, такие как:

a) техник;

b) специалист по оценке/тестированию;

c) старший специалист по оценке/тестированию;

d) ведущий специалист по оценке/тестированию.

6.2 Уровень 1 (помощник):

- обеспечивает выполнение некоторых мероприятий, требуемых методами тестирования соответствия или оценки;
- может выполнять мероприятия по тестированию и оценке под наблюдением.

6.3 Уровень 2 (профессионал):

- способен работать самостоятельно во многих областях тестирования или оценки, но может потребоваться помощь в нескольких областях;
- умеет понимать смысл отклонений, обнаруженных в отношении действий лаборатории, и реагировать на них.

6.4 Уровень 3 (менеджер):

- способен работать самостоятельно в большинстве областей тестирования или оценки;
- умеет понимать смысл и реагировать на отклонения, обнаруженные в отношении действий лаборатории;
- может контролировать работу по тестированию или оценке тех, кто находится на уровнях 1 и 2.

6.5 Уровень 4 (руководитель):

- компетентен в рассмотрении разных вариантов тестирования или оценки в соответствии с определенными стандартами и методами по крайней мере для одной технологической области;
- компетентен в общении с заинтересованными сторонами, включая регулирующие органы и производителей, и может обеспечить управление проектом для проведения оценки или тестирования соответствия;
- компетентен работать самостоятельно со всеми методами тестирования/оценки, указанными в проекте;
- умеет понимать смысл и реагировать на отклонения, обнаруженные в отношении действий лаборатории;
- может наблюдать и обеспечивать наставничество в отношении работы по тестированию/оценке сотрудников, находящихся на уровнях 1, 2 и 3.

7 Измерение элементов компетенции

7.1 Знание

Области знаний, определенные в серии стандартов ISO/IEC 19896, предоставляют измеряемую совокупность знаний для каждого стандарта обеспечения ИБ продуктов ИТ. Проверки знаний могут включать оценку профессиональных знаний, полученную от третьих лиц или в результате проверок, разработанных и проведенных уполномоченными органами или самой лабораторией.

7.2 Навыки

От специалистов по тестированию и оценке продуктов ИБ требуются различные навыки, которые представлены в последующих частях серии ISO/IEC 19896. Эти навыки должны быть измеряемыми.

Примеры методов измерения навыков включают:

- выполнение положений программы проверки квалификации лабораторий, реализуемой как часть требований по соответствию ISO/IEC 17025;
- использование записей обучения, проводимого в соответствии с ISO/IEC 17025, в детализации по мерам эффективности обучения, которые, в свою очередь, могут продемонстрировать владение навыком;
- наличие профессиональных сертификатов в отношении определенных навыков;
- обратную связь от персонала, уже признанного компетентным в том или ином навыке.

7.3 Опыт

Опыт следует измерять путем ведения учета количества завершенных проектов и их описания, включающего техническую область, с точки зрения сложности проекта, технологий и методов тестирования, используемых в проектах.

Примечание — Количество лет, проведенных на соответствующих должностях, само по себе не является адекватным показателем, поскольку опыт отражает объем и разнообразие реализованных проектов в той же степени, что и их продолжительность.

7.4 Образование

Образование и квалификация специалиста обычно подтверждаются владением подлинными сертификатами, выданными организациями, признанными уполномоченными органами.

7.5 Эффективность

Критерии измерения эффективности специалистов по тестированию и оценке должны устанавливаться лабораторией. Соответствующие критерии включают:

- время, необходимое для составления плана тестирования или оценки;
- время, необходимое для выполнения плана тестирования или оценки и его завершения;
- количество, тип и серьезность замечаний, полученных в ходе внутренней деятельности по обеспечению качества;
- количество, тип и серьезность комментариев, полученных на этапе проверки;
- возможность повторить тесты из тестовой документации, подготовленной другими компетентными специалистами по тестированию или оценке;
- способность понимать новые инструменты и технологии;
- способность объяснять ошибки и состояние тестирования производителям, проверяющим и другим членам команды;
- точность результатов оценки или тестирования;
- использование целевого и концентрированного языка в отчетах об испытаниях.

7.6 Запись элементов компетенции

ISO/IEC 17025 требует, чтобы лабораторией велись записи о компетенции. Приложения А и В предоставляют пример таблицы для записи этой информации.

Приложение А
(справочное)

Таблица для описания требований к компетенции

В таблицах с А.1 по А.4 описывается структура, которая может использоваться лабораториями для определения требований к конкретной компетенции с использованием критериев знаний, навыков, опыта и образования для каждого уровня компетенции. Информация в таблицах дополняет минимальные требования, определенные в разделе 7.

ISO/IEC 19896-2 и ISO/IEC 19896-3 предоставляют конкретные критерии компетенции для специалистов по тестированию в соответствии с ISO/IEC 19790 и специалистов по оценке в соответствии с ISO/IEC 15408, которые можно использовать при заполнении таблиц.

Таблица А.1 — Описание требований к компетенции для уровня 1 (помощник)

Уровень 1 (помощник)	
Наименование области знаний	Описание области знаний
Наименование навыка	Описание навыка
Требуемый опыт	
Требуемое образование	
Критерий эффективности	

Таблица А.2 — Описание требований к компетенции для уровня 2 (профессионал)

Уровень 2 (профессионал)	
Наименование области знаний	Описание области знаний
Наименование навыка	Описание навыка
Требуемый опыт	
Требуемое образование	
Критерий эффективности	

Таблица А.3 — Описание требований к компетенции для уровня 3 (менеджер)

Уровень 3 (менеджер)	
Наименование области знаний	Описание области знаний
Наименование навыка	Описание навыка
Требуемый опыт	
Требуемое образование	
Критерий эффективности	

Таблица А.4 — Описание требований к компетенции для уровня 4 (руководитель)

Уровень 4 (руководитель)	
Наименование области знаний	Описание области знаний
Наименование навыка	Описание навыка
Требуемый опыт	
Требуемое образование	
Критерий эффективности	

Приложение В
(справочное)

Примеры описания опыта и компетенции

В таблице В.1 приведен пример структуры для описания опыта, полученного специалистом по оценке в соответствии с ISO/IEC 15408 или специалистом по тестированию в соответствии с ISO/IEC 19790.

Возможно, что в последующих частях серии ISO/IEC 19896 будут указаны более конкретные примеры описания опыта и компетенции.

Лаборатории должны разработать метод определения сложности проекта на основе своего опыта ведения проектов.

Например, «простой» и «комплексный» оценочный уровень доверия для оценок, полученных в соответствии с ISO/IEC 18045 или уровень безопасности криптографического модуля, оцененный по ISO/IEC 24759.

Таблица В.1 — Пример описания опыта

Описание опыта					
Имя специалиста по тестированию/оценке					
Идентификатор проекта	Сроки проекта	Область технологий	Сложность проекта	Количество часов работы над проектом	Примененные методы тестирования/оценки

В таблице В.2 представлен пример структуры для описания компетенции, полученной специалистом по оценке в соответствии с ISO/IEC 15408 или специалистом по тестированию ISO/IEC 19790.

Возможно, что в последующих частях серии ISO/IEC 19896 будут представлены другие примеры описания.

Таблица В.2 — Пример описания компетенции

Описание компетенции					
Имя специалиста по тестированию/оценке					
Идентификатор проекта	Опыт	Знания	Навыки	Эффективность	Уровень компетенции

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO/IEC 17000	IDT	ГОСТ ISO/IEC 17000-2012 «Оценка соответствия. Словарь и общие принципы»
ISO/IEC 17025	IDT	ГОСТ ISO/IEC 17025-2019 «Общие требования к компетентности испытательных и калибровочных лабораторий»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT — идентичные стандарты.		

Библиография

[1] ISO/IEC 15408 (all parts), Information technology — Security techniques — Evaluation criteria for IT security

[2] ISO/IEC 15443, Information technology — Security techniques — Security assurance framework

[3] ISO/IEC 17024, Conformity assessment — General requirements for bodies operating certification of persons

[4] ISO/IEC/TS 17027, Conformity assessment — Vocabulary related to competence of persons used for certification of persons

[5] ISO/IEC 17065, Conformity assessment — Requirements for bodies certifying products, processes and services

[6] ISO/IEC 18045, Information technology — Security techniques — Methodology for IT security evaluation

[7] ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules

[8] ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules

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

Ключевые слова: информационная безопасность, менеджмент информационной безопасности, продукты информационных технологий, компетенции, оценка безопасности информационных технологий

Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 05.07.2021. Подписано в печать 12.07.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,90.

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