ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 19770-1— 2021

Информационные технологии

УПРАВЛЕНИЕ ИТ-АКТИВАМИ

Часть 1

Системы управления ИТ-активами. Требования

(ISO/IEC 19770-1:2017, IDT)

Издание официальное

Москва
Российский институт стандартизации
2021

Предисловие

1 ПОДГОТОВЛЕН Ассоциацией организаций и специалистов в сфере управления информационными технологиями «ИТ сервис-менеджмент форум» (ИТСМ ФОРУМ) 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 25 октября 2021 г. № 1289-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 19770-1:2017 «Информационные технологии. Управление ИТ-активами. Часть 1. Системы управления ИТ-активами. Требования» (ISO/IEC 19770-1:2017 «Information technology — IT asset management — Part 1: IT asset management systems — Requirements», IDT).

ИСО/МЭК 19770-1:2017 разработан подкомитетом ПК 7 «Программная и системная инженерия» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК)

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 19770-1—2014

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.rst.gov.ru)

Содержание

Введение

Настоящий стандарт определяет требования к созданию, внедрению, обслуживанию и совершенствованию системы управления ИТ-активами.

В настоящем стандарте изложены дополнительные требования к ИСО 55001:2014 «Управление активами. Национальная система стандартов. Система менеджмента. Требования», в котором указаны требования к созданию, внедрению, сопровождению и совершенствованию системы управления активами. В настоящем стандарте изложены дополнительные или более подробные требования, которые считаются необходимыми для управления ИТ-активами. Основным отличием является необходимость управления программными активами с их особыми характеристиками. Несмотря на то, что ИСО 55001:2014 может быть использован для управления программными активами, если организации надлежащим образом определяют их область применения и предъявляют соответствующие требования, ИСО 55001:2014 в первую очередь ориентирован на физические активы, с незначительным фокусом на управление программными активами.

Существует ряд характеристик ИТ-активов, для которых необходимы эти дополнительные или более подробные требования. Они описаны в приложении С. В результате появления таких характеристик ИТ-активов, к системе управления ИТ-активами, следовательно, будут предъявляться явные требования, дополнительно к тем, что определены в ИСО 55001:2014, касающиеся:

- контроля модификации, дублирования и распространения программного обеспечения, с особым вниманием к контролю доступа и целостности;
- аудиторской прослеживаемости авторизаций и изменений, внесенных в ИТ-активы;
- контроля лицензирования, недостаточного лицензирования, избыточного лицензирования и соблюдения условий лицензирования;
- контроля ситуаций, связанных со смешанным владением и ответственностью, например в облачных вычислениях и с практикой «принести свое собственное устройство» (BYOD);
- сверки данных управления ИТ-активами с данными в других информационных системах, если это оправдано ценностью для бизнеса, в частности с финансовыми информационными системами учета активов и расходов.

Кроме того, поскольку информация, связанная с ИТ-активами, как правило, является объемной, очень сложной и быстро меняющейся, вполне вероятно, что организациям с такой информацией потребуется использовать автоматизированные информационные системы.

Другое различие между ИСО 55001:2014 и настоящим стандартом состоит в том, что настоящий стандарт дополнительно обеспечивает несколько различных явных групп целей процессов (или уровней). Наиболее важным из них является базовый уровень, называемый достоверные данные, который является наиболее важным для большинства организаций конечных пользователей, а также для разработчиков программного обеспечения. Второй уровень предназначен для интеграции жизненного цикла, а третий — для оптимизации. Более подробная информация об уровнях и их соответствующих группах целей приведена в приложении В.

Поскольку основные физические активы все чаще включают в свой состав программное обеспечение или зависят от него, вполне вероятно, что дополнительные требования настоящего стандарта будут актуальны в таких ситуациях. Вполне вероятно, что большинству организаций, имеющих преимущественно физические активы, потребуются системы управления, отвечающие сочетанию «чистых» требований ИСО 55001: 2014 с дополнительными требованиями настоящего стандарта.

ИТ-активы охватывают широкий спектр типов активов. На рисунке 1 схематически показаны основные типы ИТ-активов.

Настоящий стандарт может использоваться любой организацией и может применяться ко всем типам ИТ-активов. Организация определяет, к какому из ее ИТ-активов относится настоящий стандарт.

Настоящий стандарт, в первую очередь, предназначен для использования:

- теми, кто участвует в создании, внедрении, сопровождении и совершенствовании системы управления ИТ-активами;
- теми, кто занимается предоставлением услуг по управлению ИТ-активами, включая поставщиков услуг;
- внутренними и внешними сторонами для оценки способности организации соответствовать юридическим, нормативным и договорным требованиям и собственным требованиям организации.

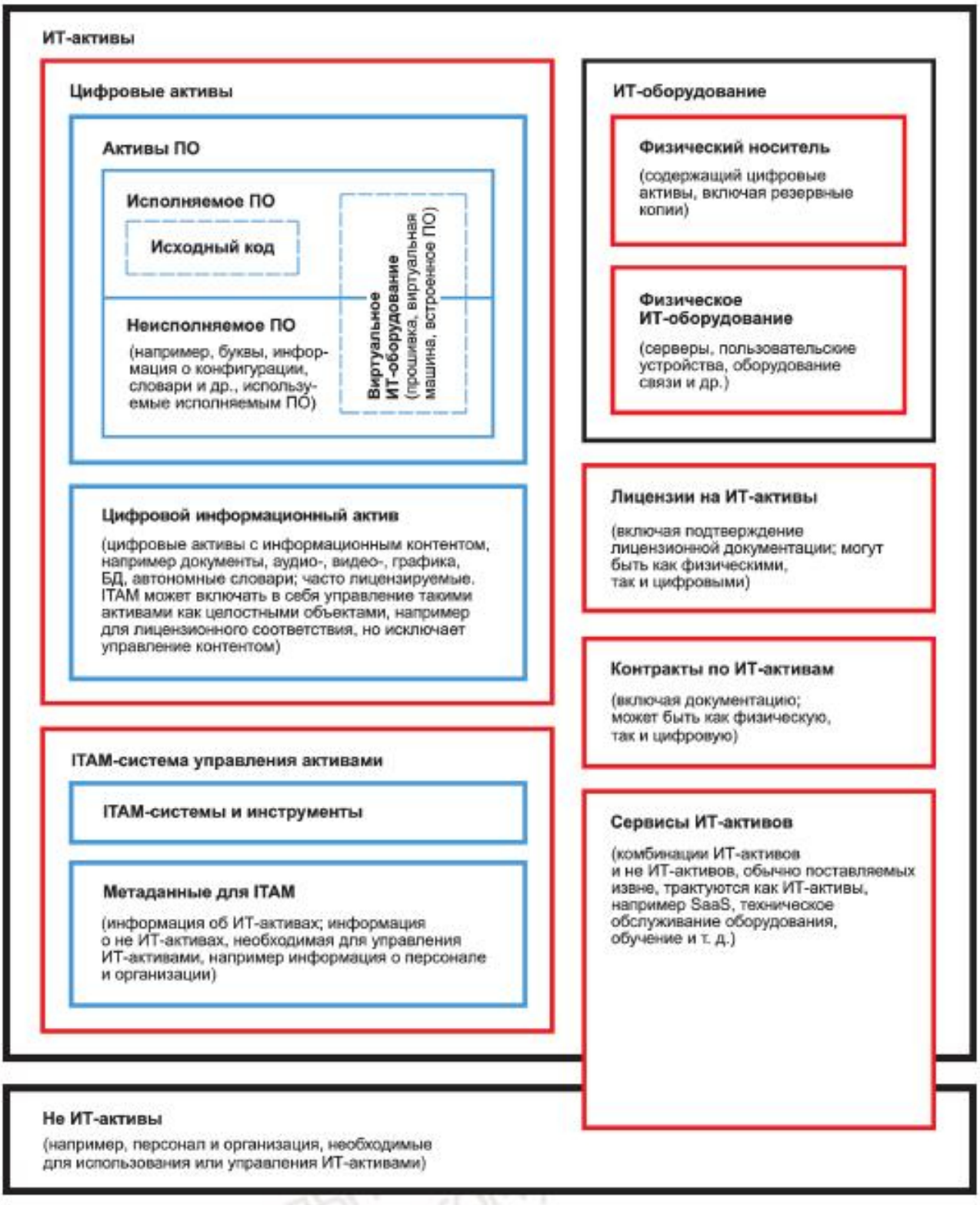

Рисунок 1 — Основные типы ИТ-активов

Порядок, в котором требования представлены в настоящем стандарте, не отражает их важность и не подразумевает порядок, в котором должно обеспечиваться их выполнение.

Дальнейшие рекомендации, касающиеся исполнения требований, определенных настоящим стандартом, совместно с ИСО 55001:2014, приведены в ИСО 55002.

Общая информация об управлении активами и об управлении ИТ-активами, а также информация о терминологии, используемой в настоящем стандарте, представлена в ИСО 55000 и ИСО/МЭК 19770-5 «Управление активами. Национальная система стандартов. Общее представление, принципы и терминология» и в ИСО/МЭК 19770-5.

В настоящем стандарте применяется термин «риск», определенный в ИСО 31000:2009 «Менеджмент риска. Принципы и руководство» и в Руководстве ИСО/МЭК 73:2009. Кроме того, используется термин «акционер» вместо термина «заинтересованное лицо».

Настоящий стандарт предназначен для того, чтобы позволить организации согласовать и интегрировать свою систему управления ИТ-активами с соответствующими требованиями к системе управления, например указанными в ИСО/МЭК 27001 и ИСО/МЭК 20000-1.

Настоящий стандарт не должен противоречить каким-либо политикам, процедурам и стандартам организации. Любой такой конфликт должен быть разрешен перед использованием настоящего стандарта.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

УПРАВЛЕНИЕ ИТ-АКТИВАМИ

Часть 1

Системы управления ИТ-активами. Требования

Information technology. IT asset management. Part 1. IT asset management systems. Requirements

Дата введения — 2022—04—30

1 Предметная область

1.1 Назначение

В настоящем стандарте указаны требования к системе управления ИТ-активами в контексте организации.

Настоящий стандарт может быть применен организациями всех типов и размеров ко всем типам ИТ-активов.

Примечания

1 Настоящий стандарт, в основном, предназначен к использованию для управления ИТ-активами, но он также может применяться к другим типам активов. Он может быть полезен, полностью или частично, для управления встроенным программным обеспечением и прошивками, однако его использование для этих целей не было определено. Он не предназначен для управления информационными активами как таковыми, то есть он не предназначен для управления информацией как активом независимым от аппаратных и программных активов. Некоторые типы данных и информации охватываются, такие как данные и информация об ИТ-активах в предметной области, и в зависимости от того, как определена предметная область, она может охватывать цифровые информационные активы. См. разъяснение об ИТ-активах во введении.

2 В настоящем стандарте не представлены финансовые, бухгалтерские или технические требования для управления конкретными типами ИТ-активов.

3 В настоящем стандарте используется термин «система управления ИТ-активами» для обозначения системы управления, предназначенной для управления ИТ-активами.

Настоящий стандарт является конкретным расширением предметной области ИСО 55001:2014, с изменениями, и не является отраслевым применением данного стандарта. В основном, ИСО 55001:2014 предназначен для управления физическими активами, но он также может применяться к другим типам активов. В настоящем стандарте определены требования к управлению ИТ-активами, которые являются дополнительными к требованиям, определенным в ИСО 55001:2014. Соответствие настоящему стандарту не означает соответствия ИСО 55001:2014.

Настоящий стандарт может использоваться внутренними и внешними сторонами для оценки способности организации соответствовать собственным требованиям по управлению ИТ-активами.

1.2 Область применения

Настоящий стандарт относится к процессам управления ИТ-активами и может быть применен организациями для достижения немедленных выгод.

Настоящий стандарт может быть применен ко всем ИТ-активам. Например, он может применяться не только для ИТ-оборудования, но и для исполняемого программного обеспечения (такого как приклад-

Издание официальное

ные программы и операционные системы), а также для неисполняемого программного обеспечения (такого как шрифты и информация о конфигурации). Он может применяться ко всем технологическим средам и вычислительным платформам (например, виртуализированным программным приложениям, локальным приложениям или приложениям, предоставляемым как услуга; равно применим для облачных вычислений, и для унаследованных вычислительных сред).

1.3 Ограничения

В настоящем стандарте не детализируются процессы управления ИТ-активами с точки зрения методов или процедур, необходимых для удовлетворения требований к результатам процесса.

В настоящем стандарте не указывается последовательность шагов, которые должны выполняться организацией для реализации управления ИТ-активами.

В настоящем стандарте не детализируется документация с точки зрения наименования, формата, явного содержания и носителя записей.

2 Нормативные ссылки

В настоящем стандарте нормативные ссылки отсутствуют.

3 Термины и определения

ИСО и МЭК поддерживают терминологические базы данных, используемые для стандартизации по следующим адресам:

- Электропедия МЭК: доступна по адресу https://www.rst.gov.ru/portal/gost/home/systems/electroportal
- платформа онлайн-просмотра ИСО доступна по адресу https://www.iso.org/ru/home.html

В настоящем стандарте применены следующие термины и определения.

Некоторые из этих терминов приведены из ИСО 55000:2014 и относятся к активам в целом. Эти термины применимы для ИТ-активов при использовании в контексте управления ИТ-активами, при этом термин «актив» понимается как «ИТ-актив». В некоторых случаях добавлены термины, специфичные для ИТ-активов. Никакая конкретная интерпретация не предполагается на основе того, был ли определен термин, специфичный для ИТ, или не был определен.

3.1 **актив** (asset): Произвольный объект, предмет или сущность, которые имеют потенциальную или фактическую ценность для организации (3.38).

Примечания

1 Ценность может быть материальной или нематериальной, финансовой или нефинансовой, и включать риски (3.48) и обязательства. На разных этапах жизненного цикла (3.2) активов ценность может быть как положительной, так и отрицательной.

2 Физические активы обычно относятся к оборудованию, инвентарю и недвижимости, принадлежащим организации. Физические активы противоположны нематериальным активам, которые являются нефизическими активами, такими как аренда, бренды, цифровые активы, права на использование, лицензии, права интеллектуальной собственности, репутация или соглашения.

3 Группа активов, именуемая системой активов (3.7), также может считаться активом.

[ИСО 55000:2014, 3.2.1]

3.2 **жизненный цикл актива** (asset life): Период от создания актива (3.1) до окончания срока службы актива.

[ИСО 55000:2014, 3.2.2]

3.3 **управление активами** (asset management): Скоординированная деятельность организации (3.38) для получения ценности от активов (3.1).

Примечания

1 В получение ценности обычно входит уравновешивание расходов, рисков (3.48), возможностей и производительности (3.42).

2 К данной деятельности также относится применение элементов системы управления активами (3.5).

3 Термин «деятельность» имеет широкое значение и может включать, например, подход, планирование, планы и их реализацию.

[ИСО 55000:2014, 3.3.1]

3.4 **план управления активами** (asset management plan): Документированная информация (3.19), которая определяет виды деятельности, ресурсы и временные рамки, необходимые для отдельного актива (3.1) или группы активов, для достижения организацией (3.38) целей (3.37) управления активами (3.3).

Примечания

1 Группировка активов может осуществляться по типу актива (3.8), классу активов, системе активов (3.7) или портфелю активов (3.6).

2 План управления активами выделяется из стратегического плана управления активами (3.53).

3 План управления активами может быть включен непосредственно в стратегический план управления активами или может являться вспомогательным планом в дополнение к стратегическому плану управления активами.

[ИСО 55000:2014, 3.3.3]

3.5 **система управления активами** (asset management system): Система управления (3.33) для управления активами (3.3), функция которой заключается в определении политики управления активами (3.43) и целей управления активами (3.37).

Примечание — Система управления активами является подмножеством управления активами.

[ИСО 55000:2014, 3.4.3]

3.6 **портфель активов** (asset portfolio): Активы (3.1), которые входят в охват системы управления активами (3.5).

Примечания

1 Портфель активов обычно определяется и назначается в целях управленческого контроля. Портфели активов для физического оборудования могут быть определены по категориям (например, завод, оборудование, инструменты, земля). Программные портфели активов могут быть определены издателем программного обеспечения или платформой (например, ПК, сервер, мэйнфрейм).

2 Система управления активами может охватывать несколько портфелей активов. Когда используются несколько портфелей активов и систем управления активами, деятельность по управлению активами (3.3) должна быть скоординирована между портфелями и системами.

[ИСО 55000:2014, 3.2.4]

3.7 **система активов** (asset system): Набор активов (3.1), которые взаимодействуют, либо взаимосвязаны.

[ИСО 55000:2014, 3.2.5]

3.8 **тип актива** (asset type): Группировка активов (3.1), имеющих общие характеристики, которые выделяют эти активы в группу или класс.

Пример — Физические активы, информационные активы, нематериальные активы, критичные активы (3.15), обеспечивающие активы, линейные активы, активы информационно-коммуникационных технологий (ИКТ), инфраструктурные активы, движимые активы.

[ИСО 55000:2014, 3.2.6]

3.9 **аудит** (audit): Систематический, независимый и документированный процесс (3.46) получения свидетельств аудита и их объективной оценки для определения степени, в которой выполняются критерии аудита.

Примечания

1 Аудит может быть внутренним аудитом (первая сторона) или внешним аудитом (вторая или третья сторона), и он может быть объединенным или интегрированным аудитом (объединяющим два и более предмета аудита).

2 Внутренний аудит проводится самой организацией или внешней стороной от ее имени.

3 Термины «Свидетельство аудита» и «Критерий аудита» определены в ИСО 19011.

[ИСО 55000:2014, 3.1.1, изменено: примечание 2 к записи добавлено для соответствия с приложением SL]

3.10 **способность** (capability): Мера <в рамках управления активами> мощности и возможностей объекта (системы, лица или организации (3.38)) по достижению своих целей (3.37).

Примечание — Способности в рамках управления активами (3.3) включают в себя процессы (3.46), ресурсы, компетенции (3.11) и технологии, позволяющие эффективно и рационально разрабатывать и осуществлять планы по управлению активами (3.4) и процедуры жизненного цикла актива (3.2), а также их непрерывное совершенствование (3.13).

[ИСО 55000:2014, 3.1.2]

3.11 **компетенция** (competence): Умение применять знания и навыки для достижения намеченных результатов.

[ИСО 55000:2014, 3.1.3]

3.12 **соответствие** (conformity): Исполнение требования (3.47).

[ИСО 55000:2014, 3.1.4]

3.13 **непрерывное совершенствование** (continual improvement): Повторяющаяся деятельность по улучшению производительности (3.42).

[ИСО 55000:2014, 3.1.5]

3.14 **корректирующее действие** (corrective action): Действия по устранению причины несоответствия (3.36) и предотвращения его повторения.

Примечание — Действия, необходимые для минимизации или устранения причин и уменьшения воздействия или предотвращения повторения, в случае других нежелательных результатов, выходят за рамки данного определения.

[ИСО 55000:2014, 3.4.1]

3.15 **критичный актив** (critical asset): Актив (3.1), который может существенно повлиять на достижение целей (3.37) организации (3.38).

Примечания

1 Активы могут быть критичными для безопасности, критичными для окружающей среды или критичными для производительности (3.42) и могут относиться к законодательным и нормативным требованиям (3.47).

2 Критичные активы могут относиться к активам, которые необходимы для предоставления услуг критичным клиентам.

3 Системы активов (3.7) можно разделять на критичные аналогично отдельным активам.

[ИСО 55000:2014, 3.2.7]

3.16 **данные** (data): Факты об объекте.

Примечание — В контексте систем управления ИТ-активами (3.28) данные могут представлять собой выявленное, измеренное или записанное представление информации, прежде чем эта информация будет проанализирована, интерпретирована или обработана. Данные могут относиться к таким объектам, как факты, события, вещи, процессы или идеи, включая концепции, которые в определенном контексте имеют конкретное значение, относящееся к ИТ-активам.

[ИСО 9000:2015, 3.8.1, изменено: добавлено примечание 1, измененное по отношению к ИСО 15784-1 и ИСО/МЭК 2382]

3.17 **цифровой актив** (digital asset): ИТ-актив (3.25), выраженный электронным способом в цифровом формате.

Примечание — Цифровые активы включают в себя программные активы (3.50) и цифровые информационные активы (3.18).

3.18 **цифровой информационный актив** (digital information content asset): Цифровой актив (3.17) с информационным наполнением.

Пример — Документы, аудио-, видео-, графики, базы данных, отдельные словари; часто лицензируются.

Примечание — ITAM может включать управление этими активами как целыми объектами, например для соблюдения условий лицензии, но исключает управление контентом.

3.19 **документированная информация** (documented information): Информация, которую требуется контролировать и поддерживать организацией (3.38), и среда, в которой информация содержится.

Примечания

1 Документированная информация может быть в любом формате и носителе и из любого источника.

2 К документированной информации можно отнести:

- систему управления (3.33), включая связанные процессы (3.46);
- информацию, созданную для того, чтобы организация функционировала (документация);
- свидетельство достигнутых результатов (например, записи, ключевые показатели эффективности).

[ИСО 55000:2014, 3.1.6]

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

[ИСО 55000:2014, 3.1.7]

3.21 **аппаратное обеспечение** (hardware): Физическое оборудование, используемое для обработки, хранения или передачи компьютерных программ или данных.

[ISO/IEC/IEEE 24765:2010, 3.1278]

3.22 **инцидент** (incident): Внеплановое событие или происшествие, в результате которого наносится вред или иной ущерб.

[ИСО 55000:2014, 3.1.8]

3.23 **информация** (information): Значимые данные.

Примечания

1 В контексте систем управления ИТ-активами (3.28) информация может представлять собой данные, которые были сформированы, преобразованы, проанализированы, интерпретированы или скомпилированы и которым придается значение в соответствии с контекстом и принятыми соглашениями (условиями). Основные данные могут относиться к таким объектам, как факты, события, вещи, процессы или идеи, включая понятия, которые в определенном контексте имеют определенное значение, связанное с ИТ-активами (3.25).

2 В контексте систем управления ИТ-активами информация может записываться в цифровом или физическом виде (например, на бумаге).

[ИСО 9000:2015, 3.8.2, изменено: примечание 1 на основе изменений согласно ISO/TR 12037, ISO/TR 21089 и ИСО/МЭК 2382) и добавлено примечание 2]

3.24 **информационные технологии;** ИТ (information technology, IT): Разработка, обслуживание и использование технологий для получения, обработки, хранения и распространения цифровой информации.

Примечание — Это исключает использование технологии для получения, обработки, хранения и распространения информации, которая не является цифровой, такой как бумажная информация. Примерами информации, которая исключаются, когда она не записана в цифровой форме, являются книги, руководства, рукописи и др. Для целей настоящего определения термин «цифровой» эквивалентен термину «электронный».

3.25 **ИТ-актив** (IT asset): Элемент, вещь или сущность, которые могут использоваться для получения, обработки, хранения и распространения информации (цифровых данных), которая имеет потенциальную или фактическую ценность для организации.

Примечания

1 ИТ-активы включают:

- программное обеспечение (3.49);
- носители (физические и цифровые);
- ИТ-оборудование (физическое и виртуальное);
- лицензии (включая подтверждение лицензии);
- контракты;
- ITAM-системы управления ИТ-активами (включая системы и инструменты ITAM, а также метаданные, необходимые для управления всеми ИТ-активами).

2 Услуги (сервисы) для отражения требований (3.47) к управлению ИТ-активами (3.26), предоставляемые внешним поставщиком услуг, также могут рассматриваться как ИТ-активы, например такие, как «программное обеспечение как услуга», техническое обслуживание оборудования, поддержка программного обеспечения, обучение.

3 Цифровые информационные активы (3.18) представляют собой файлы или другие объекты с информационным содержанием, которые не являются программным обеспечением. Например, может существовать набор стандартов в цифровой форме; набор носителей информации; рейтинговая информация кредитных агентств. Такие активы могут быть лицензированы и, следовательно, могут также рассматриваться в рамках дисциплины управления ИТ-активами.

4 Информация сама по себе, независимо от аппаратных и программных средств ИТ, может считаться активом (3.1), но она не считается ИТ-активом.

5 Связанный набор ИТ-активов также называют ИТ-инфраструктурой (3.30).

3.26 **управление ИТ-активами;** ITAM (IT asset management, ITAM): Скоординированная деятельность организации (3.38) по получению ценности от ИТ-активов (3.25).

3.27 **план управления ИТ-активами** (IT asset management plan): Задокументированная информация (3.19), определяющая виды деятельности, ресурсы и временные рамки, требуемые для управления каждым ИТ-активом (3.25) (или группой ИТ-активов), предназначенная для достижения целей (3.37) управления ИТ-активами (3.26) организации (3.38).

Примечания

1 Группировка активов может производиться по типу активов (3.8), классу активов, системам активов (3.7) или портфелю активов ИТ (3.29).

[ИСО/МЭК 19770-1:2017]

2 План управления ИТ-активами является производным от стратегического плана управления ИТ-активами (3.54).

3 План управления ИТ-активами может содержаться, или быть вспомогательным, в стратегическом плане управления ИТ-активами.

[ИСО 55000:2014, 3.3.3, изменено: план управления активами изменен на план управления ИТ-активами, все примечания приведены с учетом специфики упоминаемых дисциплин]

3.28 **система управления ИТ-активами;** ITAMS (IT asset management system, ITAMS): Система управления (3.33), обеспечивающая управление ИТ-активами (3.26), функции которой задают (определяют) политики (3.43) и цели (3.37) управления ИТ-активами.

3.29 **портфель ИТ-активов** (IT asset portfolio): ИТ-активы (3.25), которые находятся в области применения системы управления ИТ-активами (3.28).

Примечания

1 Портфель ИТ-активов определяется и назначается для обеспечения аспектов управления активами соответствующего типа. Портфели для аппаратных средств ИТ могут быть определены по категориям, например: серверы, персональные компьютеры, мобильные устройства и т. д. Портфели программных средств могут быть определены по производителю программного средства или по платформе, например: персональные компьютеры, сервера, мейнфреймы и т. д.

2 Система управления ИТ-активами может охватывать несколько портфелей ИТ-активов.

3 См. также 3.6 «Портфель активов».

3.30 **ИТ-инфраструктура** (IT infrastructure): Комплекс ИТ-активов (3.25) для разработки, обслуживания и использования ИТ сервисов (услуг).

3.31 **уровень сервиса** (level of service): Параметры или комбинация параметров, которые отражают социальные, политические, экологические и экономические результаты (эффекты), которых достигает организация (3.38).

Примечание — Параметры уровня сервисов могут содержать: безопасность, удовлетворенность клиента, качество, количество, объем, надежность, скорость реагирования, соответствие экологическим нормам, стоимость и доступность сервиса (услуг).

[ИСО 55000:2014, 3.3.6]

3.32 **жизненный цикл** (life cycle): Этапы, включенные в управление активом.

Примечания

1 Наименование и количество этапов, процессов и видов деятельности внутри каждого этапа обычно различаются в зависимости от отраслевой принадлежности и определяются организацией (3.38).

[ИСО 55000:2014, 3.2.3]

3.33 **система управления** (management system): Набор связанных или взаимодействующих между собой элементов организации (3.38) для определения политик (3.43) и целей (3.37) и процессов (3.46) организации, для достижения целей организации.

Примечания

1 Система управления может относиться к одной или нескольким областям.

2 Элементы системы включают в себя структуру организации, функции и обязанности, планирование, операционный контроль и т. д.

3 Система управления может охватывать как организацию в целом, так и отдельные или определенные функции организации, отдельные или определенные подразделения организации или одну или более функций в группе организаций.

[ИСО 55000:2014, 3.4.2, с дополнением в примечании 3 в соответствии с Annex SL]

3.34 **измерение** (measurement): Процесс (3.46) измерения для определения значений.

[ИСО 55000:2014, 3.1.10]

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

Примечания

1 Для определения состояния может возникнуть необходимость в проверке, надзоре или критической оценке.

2 Для целей управления активами мониторинг может также использоваться для определения статуса актива. Как правило, это относится к мониторингу состояния или мониторингу производительности.

[ИСО 55000:2014, 3.1.9]

3.36 **несоответствие** (nonconformity): Невыполнение требования (3.47).

3.37 **цель** (objective): Результат, который должен быть достигнут.

3.38 **организация** (organization): Лицо или группа лиц, имеющие собственные функции и ответственность, полномочия и связи для достижения своих целей (3.37).

Примечание — Концепция организации включает, но не ограничивается ими, следующие сущности: индивидуальный предприниматель, компания, корпорация, фирма, предприятие, орган власти, партнерство, благотворительное общество или учреждение, часть или комбинацию перечисленного, объединение или нет, публичное или частное.

[ИСО 55000:2014, 3.1.13]

3.39 **цель организации** (organizational objective): Всеобъемлющая цель (3.37), которая устанавливает контекст и направление для деятельности организации (3.38).

Примечание — Цели организации устанавливаются в рамках деятельности по стратегическому планированию деятельности организации.

[ИСО 55000:2014, 3.1.14]

3.40 **план организации** (organizational plan): Документированная информация (3.19), которая определяет программы для достижения целей организации (3.39).

[ИСО 55000:2014, 3.1.15]

3.41 **передать на аутсорсинг** [outsource (verb)]: Создать условия, при которых внешняя организация (3.38) выполняет часть функции или процесса (3.46) организации.

Примечание — Внешняя организация не входит в область применения системы управления (3.33), хотя переданные на аутсорсинг внешней организации функция или процесс входят в область применения, если они влияют на результативность системы управления активами (3.5).

[ИСО 55000:2014, 3.1.16]

3.42 **производительность** (performance): Измеримый результат.

Примечания

1 Производительность может относиться к количественным или качественным оценкам.

2 Производительность может иметь отношение к управлению видами деятельности, процессами (3.46), продуктами (включая услуги), системами или организациями (3.38).

3 Для целей управления активами (3.3) производительность может относиться к активам (3.1) в части их способности выполнять требования (3.47) или достигать целей (3.37).

[ИСО 55000:2014, 3.1.1]

3.43 **политика** (policy): Намерения и курс организации (3.38), официально сформулированные ее высшим руководством (3.55).

[ИСО 55000:2014, 3.1.18]

3.44 **прогнозирующее действие** (predictive action): Действие по мониторингу состояния актива (3.1) и прогнозированию необходимости предупреждающего действия (3.45) или корректирующего действия (3.14).

Примечание — Прогнозирующее действие также часто относят к «мониторингу технического состояния», к «мониторингу производительности».

[ИСО 55000:2014, 3.3.5]

3.45 **предупреждающее действие** (preventive action): Действие по устранению причины потенциального несоответствия (3.36) или иной нежелательной потенциальной ситуации.

Примечания

1 Это определение применимо только для деятельности по управлению активами (3.3).

2 Потенциальное несоответствие может иметь несколько причин.

3 Предупреждающее действие предпринимают для предотвращения возникновения несоответствия и сохранения функции актива (3.1), тогда как корректирующее действие (3.14) предпринимают для предотвращения его повторения.

4 Предупреждающее действие, как правило, выполняется в период, когда актив функционирует, или готов к функционированию, или до момента начала возникновения функционального отказа.

5 Предупреждающее действие включает пополнение расходных материалов там, где расходование материалов является функциональным требованием (3.47).

[ИСО 55000:2014, 3.3.4]

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

[ИСО 55000:2014, 3.1.19]

3.47 **требование** (requirement): Потребность или ожидание, которые установлены, обычно подразумеваются или являются обязательными.

Примечания

1 «Обычно подразумеваемый» означает, что это общепринятая или специфическая практика для организации (3.38) и заинтересованных сторон (3.52), когда рассматриваемые потребности или ожидания подразумеваются.

2 Установленным является такое требование, которое изложено, например, в документированной информации (3.19).

[ИСО 55000:2014, 3.1.20]

3.48 **риск** (risk): Влияние неопределенности на цели (3.37).

Примечания

1 Влияние — это отклонение от того, что ожидается (положительное и/или отрицательное).

2 Цели могут иметь различные аспекты (например, финансовые и экологические цели и цели в отношении здоровья и безопасности) и могут применяться на различных уровнях (стратегических, в масштабах организации, проекта, продукта или процесса (3.46)).

3 Риск часто характеризуется ссылкой на потенциально возможные «события» (как определено в Руководстве ИСО 73:2009, статья 3.5.1.3) и «последствия» (как определено в Руководстве ИСО 73:2009, статья 3.6.1.3) или их комбинации.

4 Риск часто выражают в виде комбинации последствий событий (включая изменения в обстоятельствах) и связанной с этим вероятности или возможности наступления (как определено в Руководстве ИСО 73:2009, статья 3.6.1.1).

5 Неопределенность — это состояние, заключающееся в недостаточности, даже частичной, информации, понимания или знания относительно события, его последствий или возможности его наступления.

[ИСО 55000:2014, 3.1.21, изменено: добавлено примечание 4 для соответствия с приложением SL]

3.49 **программное обеспечение** (software): Все или часть программ, которые обрабатывают или поддерживают обработку цифровой информации.

Примечания

1 Для целей данного определения программное обеспечение исключает саму информацию, такую как содержание документов, аудио- и видеозаписей, графики и баз данных.

2 Существует как исполняемое, так и неисполняемое программное обеспечение. Цель неисполняемого программного обеспечения — контролировать или поддерживать исполняемое программное обеспечение, и включает в себя, например, информацию о конфигурации, шрифты и словари для проверки орфографии. Цифровая информация, управляемая исполняемым программным обеспечением (например, содержимое документов и баз данных), не считается программным обеспечением для целей данного определения, даже если выполнение программы может зависеть от значений данных.

3.50 **программный актив** (software asset): Программное обеспечение (3.49), которое несет потенциальную или фактическую ценность для организации.

Примечание — Программное обеспечение может быть совокупностью компонентов программного обеспечения, например программный продукт может быть сборником тысяч файлов программного обеспечения.

3.51 **управление программными активами;** SAM (software asset management, SAM): Скоординированная деятельность организации по реализации ценности программных активов (3.50).

Примечания

1 Управление программными активами является специализированной частью управления ИТ-активами (3.26), ориентированной именно на активы ПО. Управление программными активами может включать управление активами, не относящимися к программному обеспечению.

2 Для справки, соответствующее отраслевое определение — это «вся инфраструктура и процессы, необходимые для эффективного управления, контроля и защиты программных активов внутри организации на всех этапах их жизненного цикла».

3.52 **заинтересованная сторона** (stakeholder): Лицо или организация (3.38), которая может воздействовать, или подвергаться воздействию, или считает, что может подвергаться воздействию решений или деятельности.

Примечание — «Заинтересованная сторона» может также упоминаться как «вовлеченная сторона».

[ИСО 55000:2014, 3.1.22]

3.53 **стратегический план управления активами;** SAMP (strategic asset management plan, SAMP): Документированная информация (3.19), которая устанавливает, как цели организации (3.39) будут преобразованы в цели (3.37) управления активами, и устанавливает подход к разработке планов управления активами (3.4) и роль системы управления активами (3.5) в обеспечении достижения целей управления активами.

Примечания

1 Стратегический план управления активами является производным от плана организации (3.40).

2 Стратегический план управления активами может быть составной частью или дополнением плана организации.

[ИСО 55000:2014, 3.3.2]

3.54 **стратегический план управления ИТ-активами** (strategic IT asset management plan): Документированная информация (3.19), которая устанавливает, как цели организации (3.39) будут преобразованы в цели (3.37) управления ИТ-активами (3.26), устанавливает подход к разработке планов управления ИТ-активами (3.27) и роль системы управления активами (3.28) в обеспечении достижения целей управления активами.

Примечания

1 Стратегический план управления ИТ-активами является производным от плана организации (3.40).

2 Стратегический план управления ИТ-активами может быть составной частью или дополнением плана организации.

[ИСО 55000:2014, 3.3.2, изменено: термин и определение стали специфическими отраслевыми]

3.55 **высшее руководство** (top management): Лицо или группа лиц, осуществляющих руководство и управление организацией (3.38) на высшем уровне.

Примечания

1 Высшее руководство наделяет полномочиями и выделяет ресурсы внутри организации.

2 Если область применения системы управления (3.33) охватывает только часть организации, то термин «высшее руководство» относится к тем лицам, которые руководят и управляют этой частью организации. Если используются несколько систем управления активами (3.5), следует обеспечить координацию их деятельности.

[ИСО 55000:2014, 3.1.23]

3.56 **достоверные данные** (trustworthy data): Данные (3.16) и связанная с ними информация (3.23), которые точны, полноценны, подходящи, легко понятны и доступны уполномоченным пользователям, которым они нужны для выполнения какой-либо задачи.

4 Контекст организации

4.1 Понимание организации и ее контекста

Организация должна определить внешние и внутренние проблемы, имеющие отношение к ее назначению и влияющие на способность организации достичь результатов, определенных для своей системы управления ИТ-активами.

Примечание — Определение этих проблем относится к установлению контекста организации, рассмотренного в ИСО 31000, подраздел 5.3.

Цели управления ИТ-активами, включенные в стратегический план управления ИТ-активами, должны быть согласованы с целями организации и соответствовать им.

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должна определить:

- заинтересованные стороны, имеющие отношение к системе управления ИТ-активами.

Примечания

1 Заинтересованные стороны включают в себя ответственных за соответствующие системы и процессы, такие как управление информационной безопасностью и управление услугами.

2 Заинтересованные стороны включают в себя лицензиаров программного обеспечения, если лицензионное программное обеспечение попадает в охват системы управления ИТ-активами;

- соответствующие требования и ожидания этих заинтересованных сторон в отношении управления ИТ-активами.

Примечание — Требования лицензиаров программного обеспечения включают в себя их условия лицензирования;

- критерии принятия решений по управлению ИТ-активами;
- требования заинтересованных сторон для учета финансовой и нефинансовой информации, относящейся к управлению ИТ-активами, а также для отчетности внутренней и внешней.

4.3 Определение предметной области системы управления ИТ-активами

Организация должна установить границы и применимость системы управления ИТ-активами для определения ее предметной области. Предметная область должна быть согласована со стратегическим планом управления ИТ-активами и политикой управления ИТ-активами. При определении предметной области организация должна учитывать:

- внешние и внутренние проблемы, упомянутые в 4.1;
- требования, упомянутые в 4.2;
- взаимодействие с другими системами управления, если они используются.

Организация должна определить портфель или портфели ИТ-активов, входящие в предметную область системы управления ИТ-активами.

Требования настоящего стандарта должны быть полностью применены к ИТ-активам, определенным организацией.

Предметная область должна быть доступна в виде документированной информации.

Примечание — Предметная область определяет, какие ИТ-активы покрываются системой управления ИТ-активами. Существует отдельное положение о том, какие процессные области включены в систему управления ИТ-активами. Это положение изложено в 6.2.1.

4.4 Система управления активами ИТ

Организация должна создать, внедрить, сопровождать и постоянно совершенствовать систему управления ИТ-активами, включая необходимые процессы и их взаимодействие в соответствии с требованиями, определенными в настоящем стандарте.

Организация должна разработать стратегический план управления ИТ-активами, который содержит документацию о роли системы управления ИТ-активами в поддержке достижения целей управления ИТ-активами.

5 Лидерство

5.1 Лидерство и обязательства

Высшее руководство должно продемонстрировать свое лидерство и обязательства в отношении системы управления ИТ-активами посредством:

- обеспечения определения и соответствия политики управления ИТ-активами, стратегического плана управления ИТ-активами и цели управления ИТ-активами стратегическим направлениям деятельности организации и организационным целям;
- обеспечения интеграции требований системы управления ИТ-активами с бизнес-процессами организации;
- обеспечения доступности ресурсов, необходимых для системы управления ИТ-активами;

- информирования о важности эффективного управления ИТ-активами и обеспечения соответствия требованиям системы управления ИТ-активами;
- обеспечения достижения системой управления ИТ-активами намеченных результатов;
- направления и поддержки персон во внесении собственного вклада в эффективность системы управления ИТ-активами;
- содействия кросс-функциональному сотрудничеству внутри организации;
- содействия постоянному улучшению;
- поддержки других соответствующих управленческих ролей в демонстрации их лидерства, применительно к их зонам ответственности;
- обеспечения согласованности подхода к управлению рисками при управлении ИТ-активами с общим подходом к управлению рисками в организации.

Примечание — Упоминание слова «бизнес» в настоящем стандарте может толковаться в широком смысле, чтобы обозначать те виды деятельности, которые являются основными для целей существования организации.

5.2 Политика

Высшее руководство должно установить политику управления ИТ-активами, которая:

a) соответствует целям организации;

b) обеспечивает основу для постановки целей управления ИТ-активами;

c) включает обязательства удовлетворить применимые требования;

d) включает обязательства постоянного совершенствования системы управления ИТ-активами.

Политика управления ИТ-активами должна:

- соответствовать организационному плану;
- соответствовать другим соответствующим политикам организации, включая политики любых других систем управления, используемых организацией;
- соответствовать соответствующим стратегическим планам любых других систем управления, используемых организацией;
- соответствовать характеру и масштабу ИТ-активов организации и связанной с ними операционной деятельности;
- соответствовать обязательствам отдельных лиц и организации по контролю за ИТ-активами;
- соответствовать приемлемому использованию ИТ-активов для нужд и задач организации;
- обеспечивать исполнение политики организации в отношении условий контрактов, связанных с ИТ-активами, включая лицензирование программного обеспечения;
- быть доступной, как связанная с ИТ-активами документированная информация;
- доноситься внутри организации;
- быть доступной для всех заинтересованных сторон, в зависимости от ситуации;
- включать в себя описание штрафов за нарушение данной политики;
- исполняться, периодически пересматриваться и, если требуется, обновляться.

5.3 Роли в организации, ответственности и полномочия

Высшее руководство должно гарантировать, что обязанности и полномочия для соответствующих ролей распределены и доведены внутри организации.

Высшее руководство должно устанавливать и назначать уровень ответственности и соответствующие полномочия для:

a) создания и обновления стратегического плана управления ИТ-активами, включая цели управления ИТ-активами;

b) обеспечения поддержки системой управления ИТ-активами реализации стратегического плана управления ИТ-активами;

c) обеспечения соответствия системы управления ИТ-активами требованиям настоящего стандарта;

d) обеспечения актуальности, адекватности и эффективности системы управления ИТ-активами;

e) создания и обновления плана(ов) управления ИТ-активами (см. 6.2.4);

f) обеспечения отчетности по эффективности системы управления ИТ-активами для высшего руководства.

6 Планирование

6.1 Действия по устранению рисков и возможности для системы управления ИТ-активами

6.1.1 Общие положения

При планировании системы управления ИТ-активами организация должна учитывать проблемы, указанные в 4.1, и требования, указанные в 4.2, определять риски и возможности, которые необходимо учитывать, для:

- уверенности в том, что система управления ИТ-активами может достичь запланированных результатов;
- предотвращения или уменьшения нежелательных последствий; а также
- достижения постоянного улучшения.

Организация должна спланировать:

a) действия по устранению этих рисков и возможностей с учетом того, как эти риски и возможности могут изменяться со временем;

b) каким образом:

- интегрировать и внедрять действия в процессы своей системы управления ИТ-активами; а также
- оценить эффективность этих действий.

6.1.2 Оценка рисков ИТ-активов

Организация должна определить и применить процесс оценки рисков ИТ-активов, который:

a) устанавливает и поддерживает критерии риска ИТ-активов, которые включают:

1) критерии принятия риска; и

2) критерии для выполнения оценки рисков ИТ-активов;

b) обеспечивает, чтобы повторные оценки риска ИТ-активов давали согласованные, действительные и сопоставимые результаты;

c) идентифицирует риски ИТ-активов:

1) применяет процесс оценки рисков ИТ-активов для выявления всех соответствующих рисков, в том числе:

- a риски, связанные с потерей конфиденциальности, целостности и доступности для ИТ-активов, входящих в охват системы управления ИТ-активами;
- b риски непрерывности бизнеса;
- c риски по соответствию правовым и нормативным требованиям;
- d риски, связанные с соблюдением договорных обязательств, включая риск соответствия лицензионным соглашениям; а также

2) определяет владельцев риска.

Примечание — Риски, связанные с информацией, содержащейся в ИТ-активах, могут оцениваться в соответствии с требованиями ИСО/МЭК 27001 по оценке рисков. Руководство по проведению оценок рисков информационной безопасности приведено в ИСО/МЭК 27005;

d) анализирует риски ИТ-активов:

1) оценивает потенциальные последствия, которые могли бы возникнуть, если риски, идентифицированные в 6.1.2c)1) материализовались;

2) оценивает реальную вероятность возникновения рисков, идентифицированных в 6.1.2c)1); а также

3) определяет уровни риска;

e) оценивает риски ИТ-активов:

1) сравнивает результаты анализа рисков с критериями риска, установленными в 6.1.2a);

2) определяет приоритет проанализированных рисков для обработки рисков.

Организация должна хранить документированную информацию о процессе оценки рисков ИТ-активов.

6.1.3 Обработка рисков ИТ-активов

Организация должна определить и применить процесс обработки рисков ИТ-активов для того, чтобы:

a) выбрать надлежащие меры по снижению рисков ИТ-активов с учетом результатов оценки рисков.

Примечание — Организации могут разрабатывать меры по смягчению рисков по мере необходимости или идентифицировать их из любого источника;

b) определить все контроли, необходимые для реализации выбранного варианта(-ов) обработки рисков ИТ-активов.

Примечание — Организации могут разрабатывать контроли по мере необходимости или идентифицировать их из любого источника;

c) сформулировать план обработки рисков ИТ-активов; а также

d) получить от владельцев ИТ-активов одобрение плана обработки рисков ИТ-активов и принятие остаточных рисков ИТ-активов.

Организация должна хранить документированную информацию о процессе обработки рисков ИТ-активов.

Примечание — Процесс оценки и обработки рисков в настоящем стандарте согласуется с принципами и общими указаниями, приведенными в ИСО 31000, а также с требованиями, указанными в ИСО/МЭК 27001:2013, 6.1.2 и 6.1.3.

6.2 Цели управления ИТ-активами и планирование их достижения

6.2.1 Детализация операционных процессов управления ИТ-активами

Организация должна определить операционные процессы, которые соответствуют степени обеспечения управления, требуемой в отношении управления ИТ-активами.

Примечания

1 В приложении А приведен список рабочих процессов для управления ИТ-активами. Этот список не является исчерпывающим, и могут потребоваться дополнительные рабочие процессы.

2 Возможно, но не обязательно указывать группы процессов для включения или исключения на основе их классификации по уровням, как описано в приложении В.

6.2.2 Цели управления ИТ-активами для операционных процессов

Организация должна определить адекватные цели для операционных процессов, отмеченных 6.2.1. Цели, определенные таким образом, должны быть сопоставлены с целями, которые приведены в приложении А.

Должно быть выпущено положение о применимости, содержащее список определенных целей с обоснованием включения или исключения любой из целей, перечисленных в приложении А.

Примечания

1 Процессы и цели процессов, перечисленные в приложении А, не являются всеобъемлющими и могут потребоваться дополнительные операционные процессы и цели процессов.

2 Термин «Положение о применимости» был выбран по аналогии с положением о применимости в ИСО/МЭК 27001. Положение о применимости совместно с определением области применения (4.3) необходимы любой внутренней или внешней стороне для понимания, что охватывается системой управления ИТ-активами.

3 Возможно, но необязательно, сгруппировать процессы и цели процессов для их включения или исключения на основе классификации по их уровням, как показано в приложении В.

6.2.3 Общие цели управления ИТ-активами

Организация должна установить цели управления ИТ-активами для значимых функций и уровней.

При определении целей управления ИТ-активами организация должна учитывать требования соответствующих заинтересованных лиц, а также прочие финансовые, технические, правовые, законодательные и организационные требования в процессе планирования управления ИТ-активами.

Примечания

1 Обобщенный перечень целей управления ИТ-активами строится на целях управления ИТ-активами для операционных процессов, определенных в 6.2.2.

Цели управления ИТ-активами должны:

- быть согласованными и соответствовать целям организации.

2 Цели организации могут включать цели, связанные с энергоэффективностью и прочими соображениями экологической устойчивости:

- соответствовать политике управления ИТ-активами;
- быть установленными и обновляемыми с использованием критериев принятия решений в управлении ИТ-активами (см. 4.2);
- быть установленными и обновляемыми как часть стратегического плана управления ИТ-активами;

- быть измеримыми (если применимо);
- содержать количественные целевые показатели для обеспечения точности данных;
- учитывать применимые требования;
- отражать (в рамках возможного) вероятность высоких темпов изменений в технологии и в бизнес-окружении;
- быть контролируемыми;
- сообщаться соответствующим заинтересованным лицам; и
- пересматриваться и обновляться в соответствии с обстоятельствами.

Организация должна сохранять документированную информацию по целям управления ИТ-активами.

6.2.4 Планирование достижения целей управления ИТ-активами

Организации необходимо объединить планирование достижения целей управления ИТ-активами с прочими видами деятельности по организационному планированию, включая управление финансами, управление кадрами и другие поддерживающие функции.

Для достижения целей управления ИТ-активами организация должна создать, документировать и поддерживать план(ы) управления ИТ-активами. План(ы) управления ИТ-активами должны соответствовать политике управления ИТ-активами и стратегическому плану управления ИТ-активами.

Организация должна обеспечить учет в планах управления ИТ-активами значимых требований, приходящих извне в систему управления ИТ-активами.

При планировании достижения своих целей управления ИТ-активами организация должна определить и задокументировать:

a) метод и критерии принятия решений и приоритизации деятельности и ресурсов для выполнения плана(ов) управления ИТ-активами и для достижения целей управления ИТ-активами;

b) процессы и методы, которые должны использоваться для управления ИТ-активами в течение их жизненных циклов;

c) что будет сделано;

d) какие ресурсы потребуются;

e) кто будет ответственным;

f) когда будет исполнено;

g) как будут оцениваться результаты;

h) приемлемые временные рамки для плана(ов) управления ИТ-активами;

i) финансовые и нефинансовые последствия плана(ов) управления ИТ-активами;

j) период пересмотра планов управления ИТ-активами (см. 9.1);

k) действия по использованию возможностей, связанных с управлением ИТ-активами, с учетом того, как эти возможности могут изменяться во времени, посредством установления процессов для:

- идентификации возможностей;
- оценки возможностей;
- определения важности ИТ-активов для достижения целей управления ИТ-активами;
- осуществления подходящей обработки и мониторинга возможностей.

Примечание — ИСО 55001:2014 включает риски в этом тексте, в то время как настоящий стандарт определяет риски более широко в 6.1.2 и 6.1.3, подобно тому, как риски определены в ИСО/МЭК 27001.

7 Поддержка

7.1 Ресурсы

Организация должна определять и обеспечивать ресурсы, необходимые для разработки, внедрения, сопровождения и непрерывного улучшения системы управления ИТ-активами.

Организация должна обеспечить ресурсы, требуемые для достижения целей управления ИТ-активами и для осуществления действий, определенных в плане(-ах) управления ИТ-активами.

7.2 Компетенции

Организация должна:

- определять необходимые компетенции лиц(а), осуществляющих деятельность под контролем организации, которая влияет на эффективность ИТ-активов, на эффективность управления ИТ-активами и на эффективность системы управления ИТ-активами;
- гарантировать, что эти люди компетентны на основании соответствующего образования, обучения или опыта;

- где применимо, принимать меры для приобретения необходимой компетенции и оценивать эффективность принятых мер;
- сохранять соответствующую документированную информацию как доказательство компетенции; и
- периодически пересматривать текущие и будущие потребности и требования к компетенции.

Примечание — Применяемые действия могут включать, например, предоставление обучения, менторство или переназначение работающих в настоящее время сотрудников, а также найм или заключение контракта с компетентными людьми.

7.3 Осведомленность

Лица, которые осуществляют деятельность под контролем организации и могут оказывать влияние на достижение целей управления ИТ-активами, должны быть осведомлены:
- о политике управления ИТ-активами;
- их вкладе в эффективность системы управления ИТ-активами, включая выгоды от повышения производительности управления ИТ-активами;
- их трудовой деятельности, сопутствующих рисках и возможностях, и как они взаимосвязаны друг с другом; и
- последствиях несоответствия требованиям системы управления ИТ-активами.

7.4 Коммуникация

Организация должна определить потребность во внутренних и внешних коммуникациях, относящихся к ИТ-активам, управлению ИТ-активами и системе управления ИТ-активами, включая:
- то, что будет обсуждаться;
- когда обсуждаться;
- с кем обсуждаться;
- каким образом обсуждаться.

7.5 Информационные требования

Организация должна определить свои информационные требования для поддержки ее ИТ-активов, управления ИТ-активами, системы управления ИТ-активами и достижения ее целей в управлении ИТ-активами, а также целей организации. Требования могут включать, но не ограничиваться, финансовую, закупочную, договорную, лицензионную, техническую информацию и информацию об организации. При этом:

a) организация должна принимать во внимание:
- значимость выявленных рисков;
- сложность контроля характеристик ИТ-активов, как описано в приложении С;
- роли и ответственности в управлении ИТ-активами;
- какие измерения необходимы для определения достижения ИТ-активами того, что от них ожидается в отношении общих целей организации;
- процессы управления ИТ-активами, процедуры и действия;
- обмен информацией с заинтересованными сторонами, включая поставщиков услуг;
- воздействие качества, доступности и управления информацией на принятие организационных решений;

b) организация должна определить:
- требования к атрибутам идентифицированной информации;
- требования к качеству идентифицированной информации;
- как и когда информация должна собираться, анализироваться и оцениваться;

c) организация должна определить, внедрить и поддерживать процессы управления своей информацией;

d) организация должна определять требования для согласования финансовой и нефинансовой терминологии, относящейся к управлению ИТ-активами повсеместно в организации; и

e) организация должна гарантировать согласованность и прослеживаемость между финансовыми, техническими данными, а также другими соответствующими нефинансовыми данными в объеме, необходимом для ее соответствия законодательным и нормативным требованиям с учетом требований заинтересованных сторон и целей организации.

7.6 Документированная информация

7.6.1 Общее

Система управления ИТ-активами организации должна включать:

- документированную информацию, как требуется настоящим стандартом;
- документированную информацию для применимых законодательных и нормативных требований;
- документированную информацию, определенную организацией как необходимая для эффективности системы управления ИТ-активами, как определено в 7.5.

Примечания

1 Объем документированной информации для системы управления ИТ-активами может отличаться от одной организации к другой в связи:

- с размером организации и ее видом деятельности, процессами, продуктами и услугами;
- сложностью процессов и их взаимодействиями;
- компетентностью персонала;
- сложностью ИТ-актива(ов); и
- потребностью быть в состоянии продемонстрировать соблюдение, например, лицензионных положений и условий.

2 7.5 касается определения общих требований ИТ-системы, что является первоначальной задачей, связанной с разработкой системы управления ИТ-активами, однако требования должны периодически пересматриваться. 7.6 затрагивает конкретное подмножество такой информации, для целей обладания проверяемой информацией, т. е. контрольного следа.

7.6.2 Прослеживаемость владения и ответственности

Владение и ответственность за все ИТ-активы должны быть документированной информацией.

Примечания

1 Документация по владению и ответственности может иметь любой уровень детализации или обобщенности, который организация считает соответствующей. Там, где есть смешанные владение и ответственность, как для устройств конечного пользователя и серверов, так и для программного обеспечения и данных на этом оборудовании, как правило, будет необходима большая степень детализации документированной информации.

2 Владение и ответственность за один тип ИТ-актива могут повлечь ответственность за другой тип ИТ-актива. Например, поставщик облачного сервиса может сформировать значительное воздействие на лицензирование, если он добавляет ядра к облачному серверу, который предоставляется организации клиента в виде «Инфраструктура как сервис».

7.6.3 Контрольный след авторизаций и выполнения авторизаций

Все разрешения должны быть документально подтверждены. Документированная информация должна включать подробную информацию о том:

a) кто дал разрешение на авторизацию;

b) когда было дано разрешение на авторизацию;

c) причине(ах) выдачи разрешения на авторизацию.

Примечания

1 Не требуется наличие каких-либо конкретных типов авторизаций, если иное не определено в настоящем стандарте. Авторизации могут существовать на любом уровне детализации или обобщения, который организация сочтет целесообразным. Например, авторизации могут применяться ко всей организации, к конкретным подразделениям или группам лиц, к отдельным ИТ-активам или классам ИТ-активов. Авторизации также могут быть ограничены во времени. Кроме того, могут существовать различные классы авторизаций, такие как финансовые, классы безопасности, оперативные и управленческие.

Выполнение авторизаций должно быть задокументировано и включать в себя информацию о том:

a) кто выполнил авторизацию;

b) когда была выполнена авторизация;

c) в соответствии с каким разрешением.

2 Примером выполнения авторизаций является установка авторизованного (или с полномочиями на изменение) программного обеспечения.

7.6.4 Создание и изменение

При создании и обновлении документированной информации организация должна обеспечить надлежащие:

- идентификацию и описание (например, название, дата, автор или ссылочный номер);

- формат (например, язык, версия программного обеспечения, графика) и носители (например, бумажные, электронные); и
- оценку и утверждение пригодности и адекватности.

7.6.5 Контроль документированной информации

Документированная информация, требуемая системой управления ИТ-активами (ITAMS) и настоящим стандартом, должна контролироваться для обеспечения, что она:

a) доступна и уместна для использования, где и когда это необходимо; и

b) надлежащим образом защищена (например, от потери конфиденциальности, ненадлежащего использования или потери целостности).

Для контроля документированной информации организация должна заниматься следующими видами деятельности, где применимо:

- распространение, доступ, извлечение и использование;
- хранение и защита, включая сохранение разборчивости;
- контроль изменений (например, контроль версий); и
- сохранность и размещение.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и эксплуатации системы управления ИТ-активами, должна быть идентифицирована и надлежащим образом контролируема.

Примечание — Доступ может подразумевать разрешение только на просмотр документированной информации или разрешение на просмотр и изменение документированной информации и т. д.

8 Операционные процессы

8.1 Операционное планирование и контроль

Организация должна планировать, внедрять и контролировать процессы, необходимые для выполнения требований, и осуществлять действия, определенные в 6.1, план(ы) управления ИТ-активами, определенные в 6.2, и корректирующие и предупреждающие действия, определенные в 10.1 и 10.2, через:

- определение критериев для требуемых процессов;
- осуществление контроля процессов в соответствии с критериями;
- хранение документированной информации в объеме, необходимом для обеспечения уверенности и доказательств того, что процессы выполняются в соответствии с планом;
- обработку и мониторинг рисков с использованием подхода, описанного в 6.1.3.

8.2 Управление изменениями

Риски, связанные с любым запланированным, постоянным или временным изменением, которое может повлиять на достижение целей управления ИТ-активами, должны быть оценены до внедрения изменения.

Организация должна обеспечивать управление такими рисками в соответствии с 6.1.3.

Организация должна осуществлять контроль за планируемыми изменениями и рассматривать последствия непреднамеренных изменений, принимая при необходимости меры по смягчению любых неблагоприятных последствий.

8.3 Управление основными данными

Организация должна обеспечить, чтобы необходимые данные обо всех основных охватываемых ИТ-активах точно регистрировались и поддерживались в актуальном состоянии на протяжении всего жизненного цикла, и чтобы по всем ИТ-активам имелась документированная информация о том, авторизированы они или нет.

Примечания

1 Основные ИТ-активы включают в себя: программные активы, аппаратное обеспечение и услуги, связанные с ИТ-активами. Цифровые информационные активы (например, лицензированные аудио и видеозаписи, текстовые и PDF-документы) также считаются основными ИТ-активами, если они включены в охват процесса. В ситуациях со смешанной ответственностью (например, для облачных вычислений или BYOD) может быть целесообразно включить активы, за которые отвечают другие организации или отдельные лица, для того чтобы управлять связанными рисками, например несоответствием требованиям лицензирования.

2 Этот процесс включает проверку данных.

3 Этот процесс предоставляет информацию об ИТ-активах для поддержки эффективности и результативности других бизнес-процессов.

8.4 Управление лицензиями

Организация должна обеспечить, чтобы требуемые данные и информация о лицензиях, о связанных правах и использовании в соответствии с правами для всех ИТ-активов в охвате процесса были точно зарегистрированы в течение жизненного цикла; также организация должна обеспечить периодический аудит, оценку и верификацию требований, использования в соответствии с правами и самих прав.

Примечание — Если цифровые информационные активы включены в охват процесса и на них распространяются условия лицензирования, они также будут подладать под эти требования.

8.5 Управление безопасностью

Организация должна эффективно управлять безопасностью в рамках всей деятельности ITAM и поддерживать соответствие требованиям по безопасности, связанным с ITAM, для всех ИТ-активов, находящихся в области управления, и проводить периодическую проверку соответствия требованиям безопасности.

Примечание — Безопасность включает контроль доступа и целостности. Требования безопасности применяются не только к программному обеспечению, но и ко всем ИТ-активам, включая оборудование и информацию об ИТ-активах.

8.6 Другие процессы

Организация должна обеспечить функционирование любых других процессов, как определено в 6.2.2 «Цели управления ИТ-активами для операционных процессов», а также любых дополнительных процессов, определенных организацией.

Примечание — Этот пункт является механизмом добавления дополнительных процессов, как определено в приложениях А и В.

8.7 Аутсорсинг и услуги

Когда организация передает на аутсорсинг любую деятельность, которая может повлиять на достижение ее целей в области управления ИТ-активами, она должна оценить связанные с этим риски. Организация должна обеспечить контроль над процессами и операциями, которые были переданы на аутсорсинг.

Примечания

1 Аутсорсинговая деятельность в принципе включает услуги, предоставляемые извне. Примерами услуг, предоставляемых извне, являются программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS), а также техническое обслуживание оборудования, поддержка программного обеспечения и обучение. Однако термин «аутсорсинг», как правило, применяется к относительно всеобъемлющим наборам услуг, в то время как отдельные услуги, как правило, считаются более ограниченными по области применения.

2 Дополнительную информацию об управлении аутсорсингом и услугами см. в ИСО/МЭК 20000-1. Когда организация использует ИТ-инфраструктуру, ИТ-активы или данные и информацию с разделением ответственности между внутренней организацией и внешними поставщиками ИТ-услуг, организация должна оценить связанные с этим риски. При смешанной ответственности организация должна обеспечить контролируемость процессов и ИТ-инфраструктуры.

3 Примеры, связанные со смешанной ответственностью, заключаются в том, что разные стороны могут владеть устройствами, используемыми конечным пользователем (организация или третья сторона, например оператор мобильной связи), используемыми серверами (организация и третья сторона, например для облачных вычислений), лицензируемым программным обеспечением (принадлежащим организации или третьей стороне), а также хранимыми и обрабатываемыми данными (организации, персонала или третьей стороны).

Организация должна определить и задокументировать, как эти действия будут контролироваться и интегрироваться в систему управления ИТ-активами организации.

Организация должна определить:

a) процессы и виды деятельности, подлежащие аутсорсингу (включая область применения и границы аутсорсинговых процессов и видов деятельности и их взаимодействие с собственными процессами и видами деятельности организации);

b) последствия от смешанной ответственности (включая связанные с этим риски и то, как совместная ответственность может быть эффективно реализована с подотчетностью ответственных лиц);

c) ответственность и полномочия в организации по управлению внешними процессами и деятельностью;

d) процессы и возможности для обмена знаниями и информацией между организацией и ее поставщиком(ами) услуг по контрактам.

При аутсорсинге любой деятельности организация должна обеспечить, чтобы:

- привлеченные аутсорсинговые ресурсы соответствовали требованиям, определенным в 7.2, 7.3 и 7.6; и
- осуществление аутсорсинговой деятельности контролировалось в соответствии с 9.1.

8.8 Смешанная ответственность организации и ее персонала

Когда у организации и ее персонала смешанная ответственность за ИТ-активы (в охвате управления ИТ-активами) и за информацию, хранящуюся на этих активах, такая ответственность может повлиять на достижение целей организации по управлению ИТ-активами. В этом случае организация должна оценить связанные риски и обеспечить контроль таких ситуаций.

Примечания

1 Ситуации, связанные со смешанной ответственностью между организацией и ее персоналом, включают в себя использование сотрудниками собственных персональных устройств для деятельности организации (обычно называемое «Bring-Your-Own-Device» или «BYOD»), а также использование сотрудниками ИТ-активов организации в личных целях, как результат хранения личных данных или информации на ресурсах организации. Когда организация использует ИТ-инфраструктуру со смешанной ответственностью за ИТ-активы или данные или информацию между организацией и ее персоналом, организация должна оценить связанные риски. Организация должна обеспечить контроль процессов и ИТ-инфраструктуры, связанных с такой смешанной ответственностью.

2 Примером ситуации, связанной со смешанной ответственностью, является ответственность разных участников за используемые устройства конечного пользователя (корпоративные или личные или принадлежащие третьей стороне, такой как оператор мобильной связи), лицензируемое программное обеспечение (корпоративное, личное или третьей стороны), данные и информацию, которые хранятся и обрабатываются (корпоративно, лично или третьей стороной).

Организация должна определить и задокументировать, как эти действия будут контролироваться и интегрироваться в систему управления ИТ-активами организации. Организация должна определить:

a) процессы и виды деятельности, на которые влияет смешанная ответственность организации и персонала (включая область применения и границы затрагиваемых процессов и видов деятельности);

b) последствия смешанной ответственности (включая связанные риски и то, как смешанная ответственность может эффективно совмещаться с подотчетностью ответственных лиц);

c) обязанности и полномочия в организации по урегулированию ситуаций, связанных со смешанной ответственностью; а также

d) процессы и возможности для обмена знаниями и информацией между организацией и ее персоналом в этих ситуациях, связанных со смешанной ответственностью.

При возникновении ситуаций, связанных со смешанной ответственностью, организация должна обеспечить, чтобы:

- ресурсы со смешанной ответственностью отвечали требованиям 7.2, 7.3 и 7.6;
- эффективность деятельности со смешанной ответственностью контролировалась в соответствии с 9.1.

9 Оценка эффективности

9.1 Мониторинг, измерение, анализ и оценка

Организация должна определить:

a) что нуждается в мониторинге и измерении;

b) методы для мониторинга, измерения, анализа и оценки, которые применимы, для обеспечения достоверных результатов;

c) когда должны выполняться мониторинг и измерения;

d) когда результаты мониторинга и измерения должны быть проанализированы и оценены.

Организация должна сохранять соответствующую документированную информацию как свидетельство результатов мониторинга, измерения, анализа и оценки.

Организация должна оценивать и сообщать:

- о производительности ИТ-активов;
- эффективности управления ИТ-активами, включая финансовые и нефинансовые показатели;
- эффективности системы управления ИТ-активами.

Организация должна оценивать и сообщать об эффективности процессов управления рисками и возможностями.

Организация должна обеспечить мониторинг и измерения, позволяющие ей соответствовать требованиям 4.2.

9.2 Внутренний аудит

9.2.1 Организация должна проводить внутренние аудиты через запланированные интервалы времени, чтобы обеспечить информацию для установления того, что система управления ИТ-активами:

a) соответствует:

- собственным требованиям организации к системе управления ИТ-активами;
- требованиям настоящего стандарта;

b) эффективно внедрена и поддерживается.

9.2.2 Организация должна:

a) запланировать, установить, реализовывать и поддерживать программу(ы) аудита, включая требования к частоте, методам, ответственности, планированию и отчетности, которая должна учитывать важность соответствующих процессов и результаты предыдущих аудитов;

b) определять критерии аудита и масштаб для каждого аудита;

c) подбирать аудиторов и проводить аудиты для обеспечения объективности и беспристрастности процесса аудита;

d) обеспечить, чтобы результаты аудитов были доложены соответствующим руководителям;

e) хранить документированную информацию в качестве доказательства результатов реализации программы аудита и результатов аудита.

9.3 Управленческий обзор

Высшее руководство должно проверять систему управления ИТ-активами организации с запланированной периодичностью, чтобы обеспечить ее постоянное соответствие, адекватность и эффективность.

Управленческий обзор должен учитывать:

a) статус действий из предыдущих управленческих обзоров;

b) изменения во внешних и внутренних аспектах, имеющих отношение к системе управления ИТ-активами;

c) информацию об эффективности управления ИТ-активами, включая тенденции в:

- несоответствиях и корректирующих действиях;
- результатах мониторинга и измерений;
- результатах аудита;

d) деятельность по управлению ИТ-активами;

e) возможности для непрерывного улучшения;

f) изменения в профиле рисков и возможностей.

Результаты управленческого обзора должны включать решения, касающиеся возможностей непрерывного улучшения и любых потребностей в изменениях (см. 8.2) системы управления ИТ-активами.

Организация должна хранить документированную информацию в качестве свидетельства результатов управленческих обзоров.

10 Улучшение

10.1 Несоответствие и корректирующее действие

Когда выявляется несоответствие или происходит инцидент с ИТ-активами, с управлением ИТ-активами или с системой управления ИТ-активами, организация должна:

a) реагировать на несоответствие или инцидент и, если применимо:
- принять меры для контроля и исправить их;
- разобраться с последствиями;

b) оценить необходимость действия по устранению причин(ы) несоответствия или инцидента, чтобы они не повторялись или не происходили в другом месте, путем:
- рассмотрения несоответствия или инцидента;
- определения причин несоответствия или инцидента;
- определения того, существуют ли или могут ли возникнуть подобные несоответствия;

c) осуществить любое необходимое действие;

d) проверить эффективность любых предпринятых корректирующих действий;

e) внести изменения (см. 8.2) в систему управления ИТ-активами, при необходимости.

Корректирующие действия должны быть соразмерны последствиям произошедших несоответствий или инцидентов.

Организация должна хранить документированную информацию в качестве свидетельства:
- происхождения несоответствий или инцидента и любых последующих предпринятых действий;
- результатов любых корректирующих действий.

10.2 Профилактические действия

Организация должна разработать процессы для упреждающего выявления потенциальных сбоев в работе ИТ-активов и оценить необходимость превентивных действий.

При выявлении потенциального сбоя организация должна применить требования 10.1.

10.3 Непрерывное улучшение

Организация должна непрерывно улучшать соответствие, адекватность и эффективность управления ИТ-активами и системы управления ИТ-активами.

Приложение А
(обязательное)

Операционные процессы и цели управления ИТ-активами

В данном приложении описываются операционные процессы и цели управления ИТ-активами, которые должны рассматриваться для включения в систему управления ИТ-активами. Положение о применимости (6.2.2) документирует решения, которые включены или исключены.

Настоящее приложение используется в основной части настоящего стандарта следующим образом:

- 6.2.1 Детализация операционных процессов управления ИТ-активами;
- 6.2.2 Цели управления ИТ-активами для операционных процессов;
- Раздел 8 Операционные процессы, включая:
- 8.2 Управление изменениями;
- 8.3 Управление основными данными;
- 8.4 Управление лицензиями;
- 8.5 Управление безопасностью; и
- 8.6 Другие процессы.

Следует обратить внимание, что цели процессов для первых четырех процессов уже включены в настоящий стандарт и, следовательно, всегда должны быть включены в 8.2, 8.3, 8.4 и 8.5.

Типы процессов — это либо процессы управления жизненным циклом, либо функциональные процессы. Процессы управления жизненным циклом отражают этапы жизненного цикла самих ИТ-активов. Примерами являются приобретение, релиз и развертывание. Процессы функционального управления, напротив, как правило, применяются в отношении нескольких процессов жизненного цикла (и, следовательно, иногда используется термин «сквозные» процессы). Примерами являются управление изменениями, управление лицензиями, управление отношениями и контрактами.

На рисунке А.1 приведены процессные области по типу процесса.

Рисунок А.1 — Процессные области ITAM по типу процессов

В таблице А.1 приведены подробные цели процессов, структурированные по типу процесса.

Таблица А.1 — Цели процессов, структурированные по типу процесса

Процесс	Цели процесса
Процессы управления жизненным циклом ИТ-активов	
Спецификация	Цель процесса «Спецификация» применительно к ИТ-активам — гарантировать, что требования к активам должным образом запрошены и проанализированы, а также разработаны и оценены подходящие варианты, соответствующие этим требованиям
Приобретение	Цель процесса «Приобретение» применительно к ИТ-активам — гарантировать, что все активы, рассматриваемые в рамках процесса, приобретаются подконтрольно и должным образом регистрируются
Разработка	Цель процесса «ИТ-разработка» применительно к ИТ-активам — гарантировать, что все ИТ-активы, рассматриваемые в рамках процесса, в частности программные, разрабатываются с учетом требований ITAM
Релиз	Цель процесса «Управление релизами ИТ-активов» применительно к ИТ-активам — гарантировать, что релизы ИТ-активов, рассматриваемые в рамках процесса, планируются и производятся в соответствии с требованиями ITAM
Развертывание	Цель процесса «Развертывание ИТ-активов» применительно к ITAM — гарантировать, что развертывание и повторное развертывание ИТ-активов в рамках процесса выполняется с учетом требований ITAM
Эксплуатация	Цель процесса «Эксплуатация ИТ-активов» применительно к ITAM — гарантировать, что операционные действия по использованию ИТ-активов, рассматриваемых в рамках процесса, выполняются с учетом требований ITAM. Примечание — Процесс «Эксплуатация», который выполняется конечными пользователями и операторами, включает в себя использование ИТ-активов (например, создание резервных копий и прочие задачи по обслуживанию), мониторинг (например, исключений, а также использования и производительности) и оптимизацию (например, настройка параметров конфигурации для улучшения производительности или экономической эффективности). Здесь подразумевается существенная взаимосвязь с другими требованиями ITAMS. Например, соответствие политикам допустимого использования интегрируется с этим процессом. Многие из процессов функционального управления ИТ-активами будут интегрироваться с этим процессом, как, например, управление лицензиями для оптимизации развертывания лицензий
Вывод из эксплуатации	Цель процесса «Вывод из эксплуатации» применительно к ИТ-активам — вывести ИТ-активы из текущего использования с последующим переназначением, переработкой и удалением (где это уместно, в соответствии с политикой компании и соблюдением всех требований к ведению учета)
Процессы функционального управления ИТ-активами	
Управление изменениями	Цель процесса «Управление изменениями» — контролировать запланированные изменения и рассматривать последствия случайных изменений, принимая меры для смягчения любых неблагоприятных последствий должным образом.
Управление основными данными	Цель процесса «Управление основными данными» — гарантировать, что требуемые данные обо всех основных ИТ-активах (в области охвата процесса) точно регистрируются на протяжении всего жизненного цикла, и что имеется документированная информация по всем ИТ-активам, являются ли они авторизованными или нет. Примечания 1 Основные ИТ-активы включают в себя программные активы, ИТ-оборудование и услуги, связанные с ИТ-активами. Цифровые информационные активы (например, лицензионные аудио- и видеозаписи, текстовые и PDF-документы) также рассматриваются как ИТ-активы, если они включены в рамки процесса. В ситуациях со смешанной ответственностью (например, для облачных сред или BYOD) может потребоваться включить в охват системы управления ИТ-активы, за которые отвечают другие организации и лица, в целях управления связанными рисками, например нарушения лицензионного соответствия.

Окончание таблицы А.1

Процесс	Цели процесса
	2 Процесс включает в себя верификацию данных. 3 Этот процесс предоставляет информацию об ИТ-активах для поддержания рациональности и результативности других бизнес-процессов.
Управление лицензиями	Цель процесса «Управление лицензиями» — гарантировать, что требуемые данные и информация о лицензиях, относящихся к ним правах и объеме использования этих прав для всех ИТ-активов в рамках процесса должным образом регистрируются в течение всего жизненного цикла; периодически осуществляется аудит и верификация требований по использованию прав, соответствию используемых прав и предоставленных прав. Примечание — Если цифровые информационные активы включены в охват процесса и являются предметом лицензионных соглашений, на них также должны распространяться эти требования
Управление безопасностью	Цель процесса «Управление безопасностью» — эффективно контролировать безопасность во всей деятельности ITAM и поддерживать требования по согласованию правил безопасности, относящихся к ITAM, для всех ИТ-активов в рамках процесса, а также проводить периодические проверки на соответствие требованиям безопасности. Примечание — Безопасность включает в себя контроль доступа и целостности. Требования безопасности применяются не только к программному обеспечению, но и ко всем ИТ-активам, включая оборудование и информацию об ИТ-активах
Управление отношениями и контрактами	Цель процесса «Управление отношениями и контрактами» применительно к ИТ-активам — управление отношениями с другими организациями, внешними и внутренними, чтобы гарантировать бесперебойное предоставление качественных услуг по управлению ИТ-активами, а также управление всеми контрактами на ИТ-активы и услуги, для всех ИТ-активов в рамках процесса. Примечание — Этот процесс включает в себя проверку соответствия требованиям условий и положений контрактов (помимо тех, которые относятся к лицензионному соответствию)
Управление финансами	Цель процесса «Управление финансами» — гарантировать, что финансовые затраты и ценности, связанные с ИТ-активами, отслеживаются и регулируются, в том числе на предмет экономической эффективности
Управление уровнем услуг	Цель процесса «Управление уровнем услуг» — определять, регистрировать и управлять основными уровнями услуг, относящихся к ITAM для рассматриваемых в процессе ИТ-активов. Примечание — Процесс включает в себя проверку вспомогательной информации
Управление прочими рисками	Цель процесса «Управление прочими рисками» — контроль выявленных рисков, которые не покрываются ни одним другим процессом из группы функционального управления. Примечание — Процесс включает в себя проверку эффективности проводимого управления рисками

Приложение В
(справочное)

Уровни управления ИТ-активами

В данном приложении приведен обзор уровней, определенных для дополнительного использования совместно с настоящим стандартом.

Уровни — это просто группировки процессов из приложения А, определенные для упрощения ссылок. Уровни необязательно отражают последовательность, в которой процессы внедряются. Они были созданы в ответ на отзывы рынка о том, что многие организации, особенно малые, не смогли реалистично полностью внедрить все операционные процессы, но хотели что-то, что даст разумную гарантию того, что организация сможет достичь и поддерживать лицензионное соответствие программного обеспечения, даже если не будут достигнуты все другие потенциальные выгоды от хорошего SAM и ITAM.

Уровни, показанные на рисунке В.1:

- уровень 1. Достоверные данные

Достижение данного уровня означает знание того, что у вас есть, так что вы можете этим управлять. Предполагает наличие приемлемой гарантии лицензионного соответствия;

- уровень 2. Интеграция жизненного цикла

Достижение данного уровня означает большую результативность и экономическую эффективность на протяжении всего жизненного цикла ИТ-активов;

- уровень 3. Оптимизация

Достижение данного уровня означает повышение эффективности и результативности за счет сосредоточения внимания на сквозных областях функционального управления.

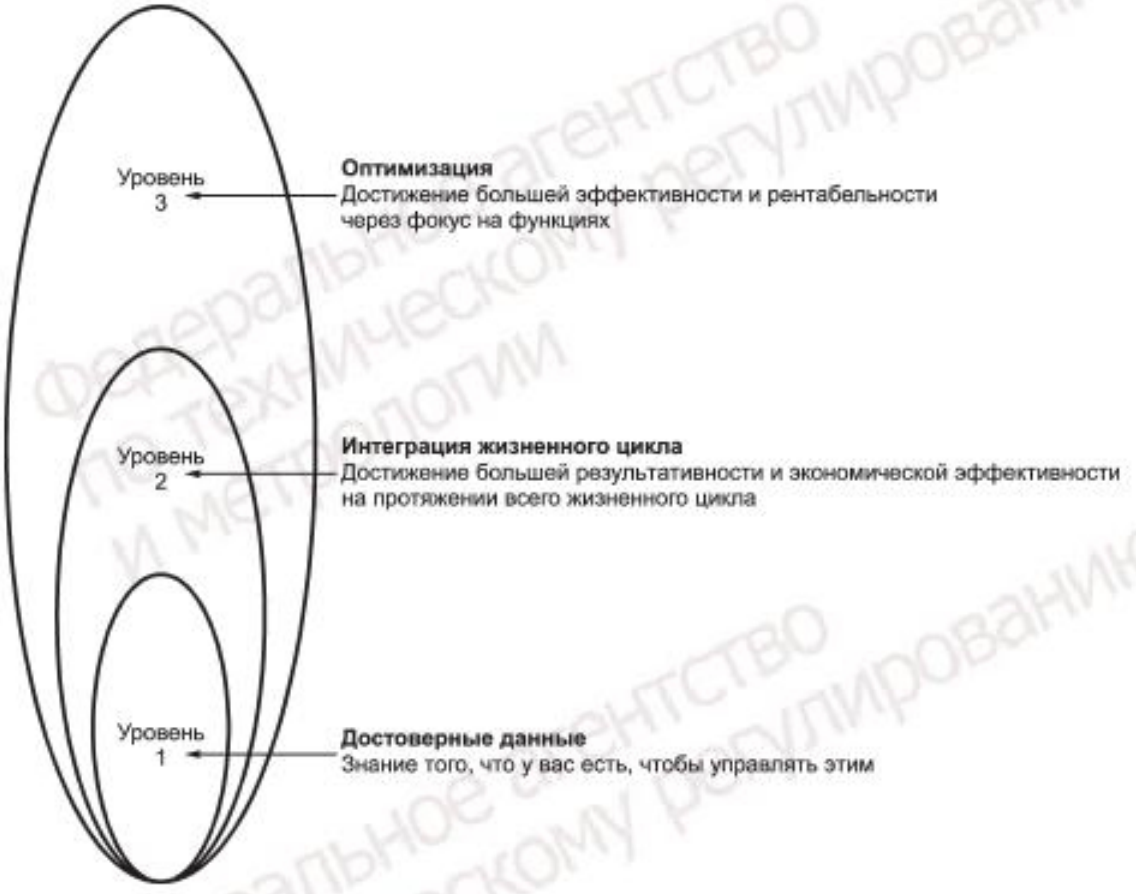

Рисунок В.1 — Уровни ITAM

Предполагается, что уровни должны быть кумулятивными, т. е. организация, которая хочет соответствовать требованиям уровня 2, также должна соответствовать требованиям уровня 1, и аналогично организация, которая хочет соответствовать требованиям уровня 3, также должна соответствовать требованиям уровней 1 и 2.

На рисунке В.2 представлен обзор процессных областей, приведенных в приложении А, по уровням.

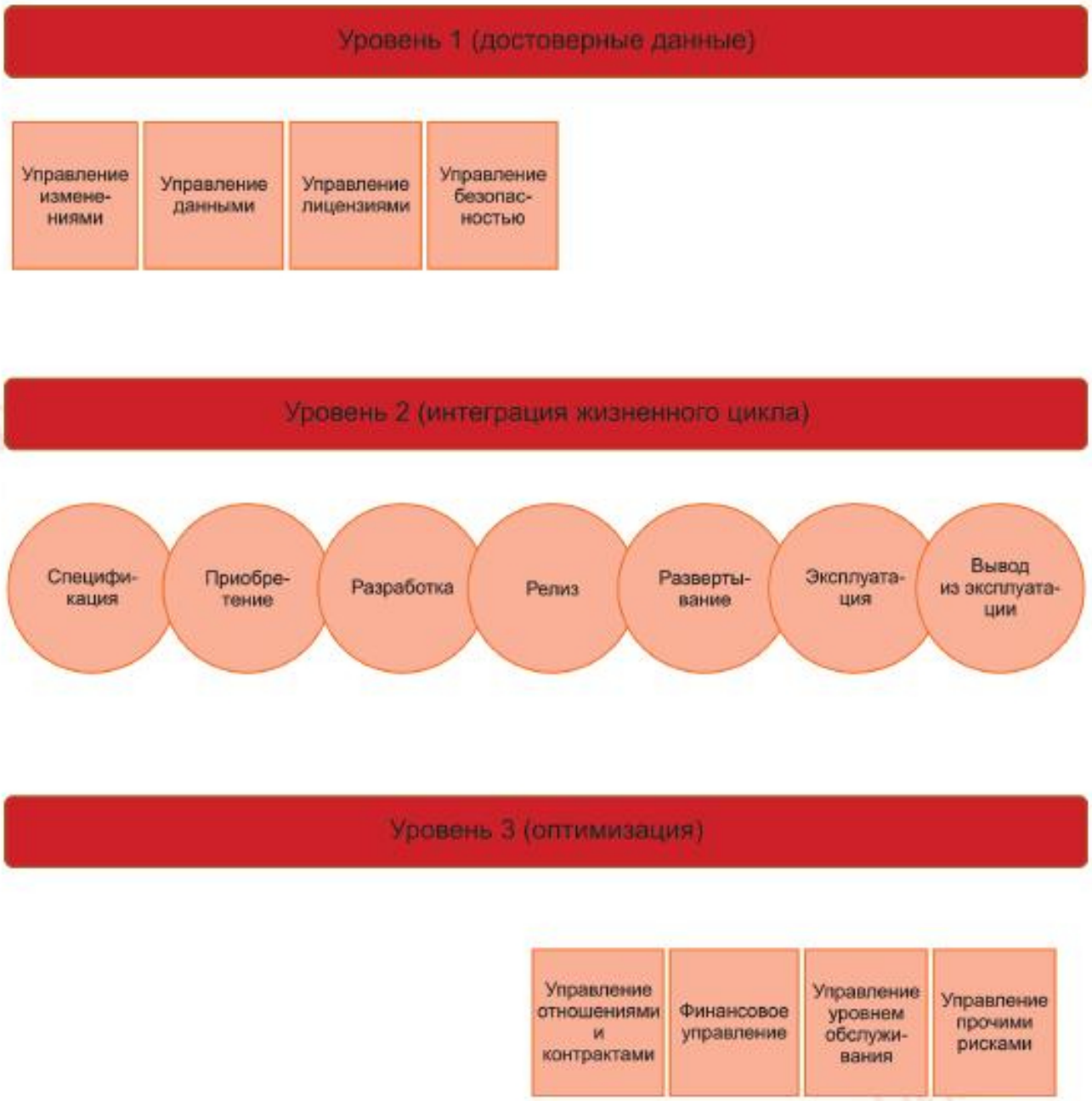

Рисунок В.2 — Процессные области ITAM по уровням

Приложение С
(справочное)

Характеристики ИТ-активов

Данное приложение содержит обзор характеристик ИТ-активов, которые создают дополнительные или более детальные требования к системе управления ИТ-активами (ITAMS) по сравнению с аналогичной для физических активов, не относящихся к ИТ. На него приводят ссылки для информации, указанной во введении, и в 7.5 (информационные требования) в качестве списка положений, которые необходимо учесть при определении информационных требований для ITAMS.

Сущность программного обеспечения. Программное обеспечение является одним из наиболее важных активов, которыми необходимо управлять в рамках управления ИТ-активами (ITAM). Оно обладает рядом характеристик, которые создают особые требования к управлению:

- **простота изменения, копирования и распространения программного обеспечения.** Поскольку программное обеспечение является электронным, а не физическим (в общепринятом смысле), оно может быть легко изменено, скопировано и распространено. Это создает значительные риски для несанкционированных (вредоносных или не вредоносных) изменений и использования программного обеспечения;
- **технологическая сложность.** Программные активы обычно сложнее физических активов во многих аспектах, таких как:
- **гибкость размещения.** Программное обеспечение может быть сохранено или установлено в одном месте, но быть задействовано или использовано из дополнительных экземпляров или мест, например с использованием виртуальных машин; для облачных сервисов, таких как программное обеспечение как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS); и обычно через сетевой доступ к программному обеспечению, размещенному на сервере;
- **количество и сложность компонентов.** Обычно программное обеспечение содержит гораздо больше компонентов, чем физические активы, например на типичном персональном компьютере могут находиться сотни тысяч файлов, а отдельные компоненты бывают очень сложны;
- **темпы изменений.** Обычно темпы изменений программного обеспечения высоки, намного выше, чем темпы изменения физических активов;
- **версии компонентов.** Существуют строгие требования к версионности программных компонентов, которая должна контролироваться для многих целей, в том числе для обеспечения безопасности, совместимости и лицензирования;
- **измерение использования.** Часто сложно измерить использование ИТ-активов, особенно программного обеспечения, что может потребоваться как в целях общего управления, так и для соблюдения контрактных обязательств. Измерение использования программного обеспечения может также зависеть от оборудования и прочих измерений, например: от процессоров или ядер; и от пользователей;
- **лицензирование.** Управление лицензированием и соблюдением условий лицензирования является основным требованием для управления программным обеспечением, которое обычно не применяется к физическим активам. Программное обеспечение, как правило, является предметом для сложных условий лицензирования. В то время как многие физические активы могут также быть предметом для условий лицензирования (например, для платежей за авторские права), иногда так бывает, что сколько разных владеющих авторскими правами (выдающих лицензию) и столько же различных условий лицензирования. Более того, сами условия лицензирования часто меняются в рамках отрасли, в рамках конкретных производителей и в рамках продуктов конкретных производителей.

Нечеткое различие между программным и аппаратным обеспечением. Физические активы, ИТ-оборудование в том числе, все чаще имеет существенные программные компоненты, которые часто представляют проблемы управления программным обеспечением даже в контекстах, типично рассматривающихся как чисто физические. Например:

- **встроенное программное обеспечение.** Физические активы все чаще имеют встроенное программное обеспечение для контроля и/или мониторинга;
- **программная реализация аппаратных функций.** Функциональность оборудования все чаще реализуется в программном обеспечении, например в платформах виртуализации и эмуляции, а также в программно-определяемых сетях;
- **носитель.** Носитель — это термин, который применяется как к физическим, так и к программным активам, причем оба типа требуют управления.

Повышенное внимание к выводу из эксплуатации/переназначению. Вывод из эксплуатации/переназначение ИТ-активов имеет более серьезный набор требований, чем для физических активов в общем. Это связано с необходимостью защиты данных, информации, и защитой от других возможных воздействий на данном этапе жизненного цикла ИТ-активов. В основном это:

- **программное обеспечение, данные и информация.** Необходимо контролировать программное обеспечение, данные и информацию ИТ-активов при выводе из эксплуатации/переназначении оборудования, например во избежание раскрытия конфиденциальной и личной информации, а также во избежание проблем соответствия с программным обеспечением;
- **электронные отходы.** В значительном числе юрисдикций существуют серьезные требования к контролю за удалением электронных отходов, вплоть до того, что они должны рассматриваться как общие требования к управлению ИТ-активами (ITAM).

Повышенные сложности управления. Существует ряд сложностей, характерных для управления ИТ-активами, которые требуют особого внимания в отношении управления этими активами, в частности:

- **смешанное владение/ответственность.** В настоящее время для ИТ-активов типично использование в смешанном режиме владения. Например, различные стороны могут владеть устройствами, используемыми конечными пользователями (организация или частные лица, или даже третья сторона), используемыми серверами (организация или третья сторона, для случая облачных вычислений), используемым программным обеспечением (организация, частные лица, третья сторона), а также данными и информацией, которые хранятся и обрабатываются (организация, частные лица или третья сторона);
- **отсутствие взаимодействия между системами ITAM и финансовыми системами.** Из-за сравнительно низких затрат на большинство ИТ-активов они обычно относятся на расходы, а не капитализируются, что приводит к серьезным сложностям для сверки между ITAM и финансовыми системами. Если эти системы не могут быть согласованы, это может подорвать доверие к ITAM со стороны финансового и управленческого персонала;
- **расхождения между технологическим обеспечением и договорными условиями.** Из-за быстро развивающихся технологических возможностей часто возникают расхождения между фактическим использованием ИТ-активов и условиями контрактов, регулирующих их использование, которые часто отстают от применяемых технологий.

Приложение D
(справочное)

Отличия от ИСО 55001

Как объяснено во введении, настоящий стандарт содержит дополнительные требования к ИСО 55001:2014, в котором указаны требования к созданию, внедрению, обслуживанию и совершенствованию системы управления для управления активами, упоминаемой как «система управления активами». Настоящий стандарт включает дополнительные или более детальные требования, которые считаются необходимыми для управления ИТ-активами.

Это достигается за счет использования в качестве основы ИСО 55001:2014, исключая только предисловие, приложения и библиографию, и за счет добавления дополнительного текста, где необходимо. (Большая часть текста из введения также продублирована.) Во введении объясняется сущность приведенных дополнений. Кроме того, также включены термины, определенные в ИСО 55000:2014.

Существует ограниченное количество случаев, где тексты ИСО 55000:2014 и ИСО 55001:2014 были изменены. К ним относятся следующие:

1 обработка риска. В настоящем стандарте принят подход к риску, используемый в ИСО/МЭК 27001:2013, который рассматривается в 6.1.2 (оценка рисков ИТ-активов) и 6.1.3 (обработка рисков ИТ-активов). Сопоставимые, но менее подробные ссылки на риск в ИСО 55001:2014 в 6.2.4 (планирование достижения целей управления ИТ-активами) были удалены, с добавлением примечания об этом;

2 обязательный текст ИСО. Ограниченное количество небольших изменений формулировок (в основном дополнений) было внесено для соответствия обязательному тексту ИСО:

a) 3.9 определение к термину «аудит»: добавлено примечание 2;
b) 3.33 определение к термину «системы управления»: добавлено одно слово;
c) 3.37 определение к термину «цель»: добавлено одно слово;
d) 3.42 определение к термину «производительности»: написание «измеримых» было исправлено;
e) 3.43 определение к термину «политики»: добавлена запятая;
f) 3.48 определение к термину «риск»: добавлен минимальный текст для соответствия приложению SL;
g) 3.52 Определение к термину «заинтересованная сторона»: изменено одно слово;
h) 4.2 Понимание потребностей и ожиданий заинтересованных сторон: ко второму перечислению добавлено одно слово;
i) 5.1 Лидерство и обязательства: к первому перечислению добавлена фраза. К третьему перечислению добавлено слово;
j) 7.3 Осведомленность: у четвертого перечисления изменилось одно слово;
k) 7.6.5 Контроль документированной информации: формулировка примечания была изменена;
l) 8.2 Управление изменениями: в третьем абзаце изменилось расположение одного слова;
m) 9.1 Мониторинг, измерение, анализ и оценка: один абзац был перенесен выше в этом пункте;
n) 9.2.2: в перечислении а) была изменена формулировка;
o) 10.1 Несоответствие и корректирующее действие: в перечислении б) была изменена формулировка.

3 Самостоятельная ссылка. Термин «этот международный стандарт», используемый в ИСО 55001:2014, был заменен на «настоящий стандарт» в настоящем стандарте.

Библиография

[1]	ISO 55001:2014	Asset management — Management systems — Requirements
[2]	ISO 9000	Quality management systems — Fundamentals and vocabulary
[3]	ISO 9001	Quality management systems — Requirements
[4]	ISO 9004	Managing for the sustained success of an organization — A quality management approach
[5]	ISO 14001	Environmental management systems — Requirements with guidance for use
[6]	ISO 19011	Guidelines for auditing management systems
[7]	ISO/IEC 19770-5	Information technology — IT asset management — Part 5: Overview
[8]	ISO/IEC 20000-1	Information technology — Service management — Part 1: Service management system requirements
[9]	ISO/IEC 20000-2	Information technology — Service management — Part 2: Guidance on the application of service management systems
[10]	ISO/IEC 27001	Information technology — Security techniques — Information security management systems — Requirements
[11]	ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls
[12]	ISO/IEC 27005	Information technology — Security techniques — Information security risk management
[13]	ISO 22301	Societal security — Business continuity management systems — Requirements
[14]	ISO 31000:2009	Risk management — Principles and guidelines
[15]	ISO 37500	Guidance on outsourcing
[16]	ISO 55000:2014	Asset management — Overview, principles and terminology
[17]	ISO 55002:2014	Asset management — Management systems — Guidelines on the application of ISO 55001
[18]	ISO Guide 73:2009	Risk management — Vocabulary
[19]	IEC 31010	Risk management — Risk assessment techniques
[20]	ASTM E2132	Standard Practice for Inventory Verification: Electronic and Physical Inventory of Assets

УДК 006.34:006.354 ОКС 35.020

Ключевые слова: информационные технологии, ИТ-активы, материальные активы, нематериальные активы, цифровые активы, программные активы, системы управления, процессы, оценка соответствия

Редактор *Н.В. Таланова*
Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 28.10.2021. Подписано в печать 23.11.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,38.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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