ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72161— 2025

Информационные технологии

УПРАВЛЕНИЕ ИТ-АКТИВАМИ

Часть 1

Системы управления ИТ-активами. Требования

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

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Публичным акционерным обществом «Газпром нефть» (ПАО «Газпром нефть») совместно с Обществом с ограниченной ответственностью «Газпромнефть Информационно-технологический оператор» (ООО «Газпромнефть ИТО»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 июня 2025 г. № 621-ст

4 Настоящий стандарт разработан с учетом нормативных положений международного стандарта 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», NEQ).

5 ВЗАМЕН ГОСТ Р ИСО/МЭК 19770-1—2021

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 (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2025

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 2
4 Контекст организации 11
4.1 Понимание организации и ее контекста 11
4.2 Понимание потребностей и ожиданий заинтересованных сторон 11
4.3 Определение предметной области системы управления ИТ-активами 11
4.4 Система управления ИТ-активами 12
5 Лидерство 12
5.1 Лидерство и обязательства 12
5.2 Политика 12
5.3 Роли в организации, ответственности и полномочия 13
6 Планирование 13
6.1 Виды планирования 13
6.2 Цели управления ИТ-активами и планирование их достижения 15
7 Поддержка 16
7.1 Ресурсы 16
7.2 Компетенции 16
7.3 Осведомленность 17
7.4 Коммуникация 17
7.5 Информационные требования 17
7.6 Документированная информация 18
8 Операционные процессы 19
8.1 Операционный контроль 19
8.2 Управление изменениями 19
8.3 Управление основными данными об ИТ-активах 20
8.4 Управление безопасностью 21
8.5 Другие процессы 21
8.6 Аутсорсинг и услуги 21
8.7 Смешанная ответственность организации и ее персонала 22
9 Оценка эффективности 22
9.1 Мониторинг, измерение, анализ и оценка 22
9.2 Внутренний аудит 23
9.3 Управленческий контроль 24
10 Улучшение 24
10.1 Несоответствие и корректирующее действие 24
10.2 Профилактические действия 24
10.3 Непрерывное улучшение 25
Приложение А (справочное) Характеристики нематериальных ИТ-активов 26
Приложение Б (справочное) Уровни зрелости управления ИТ-активами 28
Приложение В (обязательное) Процессы управления ИТ-активами 30

Введение

Настоящий стандарт определяет требования к созданию, внедрению, обслуживанию и совершенствованию системы управления информационных технологий (далее — ИТ-активы).

Кроме того, в настоящем стандарте изложены дополнительные требования помимо приведенных в ГОСТ Р 55.0.02 или более подробные требования, которые необходимы для управления ИТ-активами, в том числе материальными и нематериальными активами, с учетом особых характеристик, перечисленных в приложении А.

Примечание — Термины «материальный» и «нематериальный» добавлены с целью группировки ИТ-активов по видам.

При наличии таких характеристик ИТ-активов к системе управления ИТ-активами будут предъявляться требования в дополнение к тем, что определены в ГОСТ Р 55.0.02, касающиеся:

- контроля модификации, дублирования и распространения программного обеспечения (ПО) с акцентом на контроль доступа и целостность;
- 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 использования собственного устройства (Bring-Your-Own-Device, BYOD);
- сверки данных управления ИТ-активами с данными в других информационных системах, если это обусловлено производственной необходимостью, в частности с данными финансовых информационных систем учета активов и расходов.

Кроме того, поскольку информация, связанная с ИТ-активами, как правило, является объемной, предельно сложной и быстро меняющейся, вполне вероятно, что организациям для использования такой информации потребуются автоматизированные информационные системы.

В настоящем стандарте дополнительно представлены несколько различных уровней зрелости управления ИТ-активами, более подробная информация о которых приведена в приложении Б.

Примечание — Наименования уровней зрелости указаны согласно наименованиям уровней зрелости в приложении Б.

Так как основные физические активы все чаще включают в свой состав ПО или зависят от него, вполне вероятно, что дополнительные требования настоящего стандарта будут актуальными в таких ситуациях. Большинству организаций, имеющих преимущественно физические активы, потребуются системы управления, сочетающие требования, изложенные в ГОСТ Р 55.0.02, и дополнительные требования, приведенные в настоящем стандарте.

Настоящий стандарт может быть использован любой организацией и может быть применен как к материальным, так и нематериальным ИТ-активам. Таким образом, организация самостоятельно определяет, к какому из ее ИТ-активов относятся требования настоящего стандарта.

На рисунке 1 схематически показаны основные типы ИТ-активов.

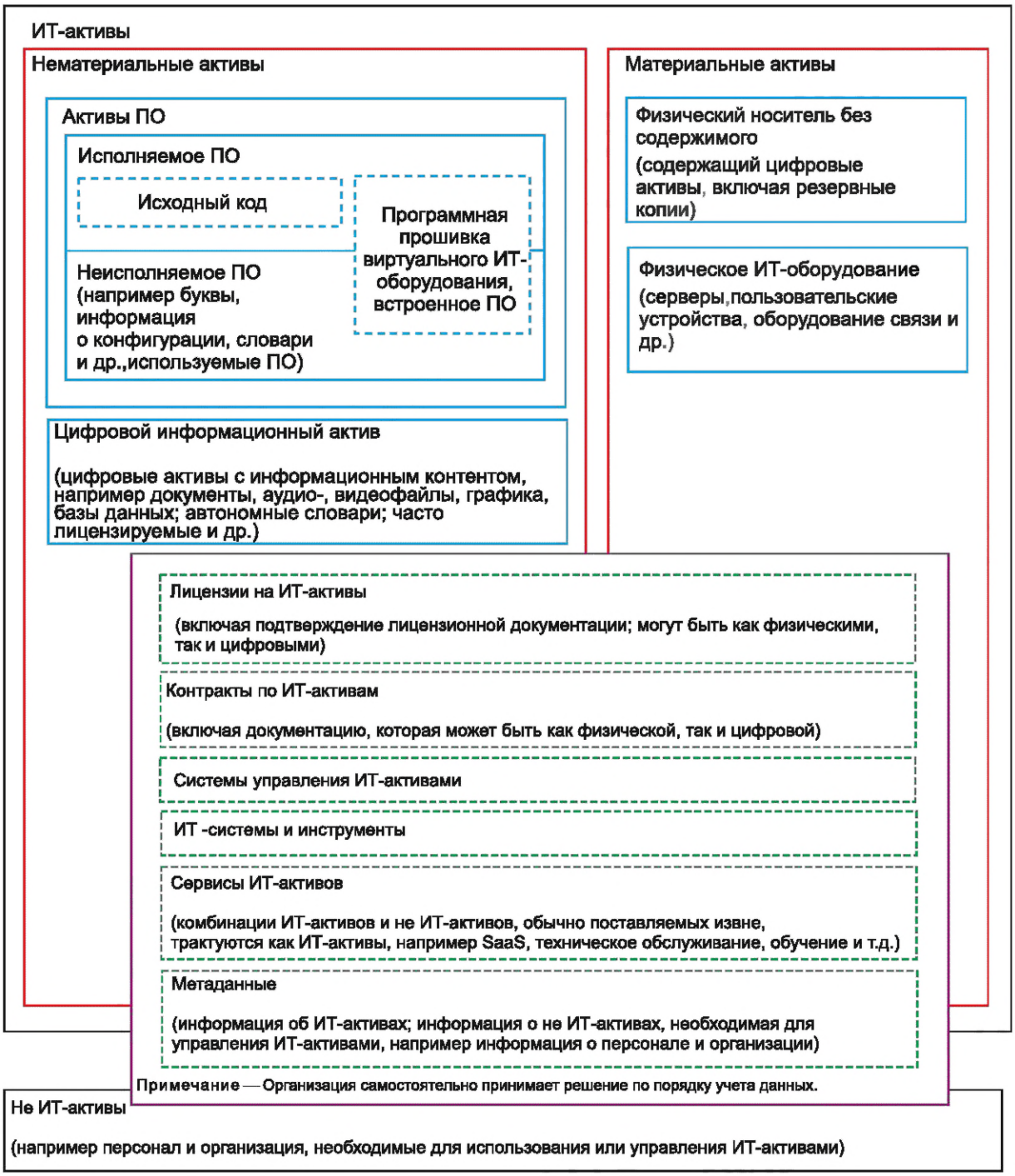


Рисунок 1 — Основные типы ИТ-активов

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.

Последовательность, в которой представлены требования в настоящем стандарте, не отражает их значимость и не подразумевает ту последовательность, в которой должно быть обеспечено их выполнение.

Рекомендации, касающиеся исполнения требований, определенных настоящим стандартом, совместно с требованиями ГОСТ Р 55.0.02 приведены в ГОСТ Р 55.0.03.

Общая информация об управлении активами и ИТ-активами, а также информация о терминологии, используемой в настоящем стандарте, представлена в ГОСТ Р 55.0.01.

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

Настоящий стандарт не должен противоречить каким-либо политикам, процедурам и стандартам организации.

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 — 2025—07—28

1 Область применения

Настоящий стандарт устанавливает требования к системе управления ИТ-активами в контексте организации.

Настоящий стандарт распространяется на организации всех типов и размеров и на все типы ИТ-активов.

Примечания

1 Настоящий стандарт, в основном, предназначен для использования при управлении ИТ-активами (материальными и нематериальными). Он может быть полезен полностью или частично для управления встроенным ПО и прошивками, однако его использование для этих целей не определено. Он не предназначен для управления информационными активами как таковыми, т. е. он не предназначен для управления информацией как активом, независимым от материальных и нематериальных 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.

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 (материальными и нематериальными).

Настоящий стандарт предназначен для описания процессов управления ИТ-активами и может быть применен организациями для достижения определенных финансовых или производственных результатов.

Настоящий стандарт распространяется на все материальные (в том числе аппаратные) и нематериальные (например, программные) ИТ-активы, в частности: ИТ-оборудование, исполняемое ПО (такое как прикладные программы и операционные системы), а также неисполняемое ПО (например, шрифты и информация о конфигурации).

Настоящий стандарт распространяется на все технологические среды и вычислительные платформы (например, виртуализированные программные приложения, локальные приложения или приложения, предоставляемые как услуга, а также облачные вычисления и унаследованные вычислительные среды).

Настоящий стандарт не распространяется на процессы управления ИТ-активами с учетом методов или процедур в соответствии с требованиями, предъявляемыми к результатам процесса.

Настоящий стандарт не распространяется на документацию с точки зрения ее наименования, формата, содержания, а также носителя записей.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 31000—2019 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО/МЭК 20000-1 Информационные технологии. Менеджмент сервисов. Часть 1. Требования к системе менеджмента сервисов

ГОСТ Р ИСО/МЭК 27001—2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1

актив (asset): Идентифицируемый предмет, вещь или объект, который имеет потенциальную или действительную ценность для организации.

Примечания

1 Ценность может быть материальной или нематериальной, монетарной или немонетарной и включать риски и обязательства. Ценность может быть положительной или отрицательной на различных этапах жизни актива.

2 К физическим активам обычно относят оборудование, запасы и объекты недвижимости, принадлежащие организации. Физические активы противоположны нематериальным активам, не имеющим физической формы, таким как права пользования нематериальными объектами, бренды, цифровые активы, права использования интеллектуальной собственности, лицензии, интеллектуальные права, репутация и деловые отношения.

3 Группа активов, составляющая систему активов, может также рассматриваться как актив.

[ГОСТ Р 55.0.01—2014, статья 3.2.1]

3.2 **атрибутный состав** (attribute composition): Необходимые признаки, принадлежность, характеризующие свойства ИТ-активов.

Примечание — Предназначен для ИТ-активов, используемых внутри организации, в зависимости от потребности в соответствии с утвержденной системой управления ИТ-активами.

3.3 **аудит** (audit): Независимая систематическая проверка и оценка данных об ИТ-активах и процессах, системах управления ИТ-активами на предмет соответствия установленным критериям оценки, подлежащие обязательному документированию в процессе проведения с последующим предоставлением отчетной документации.

Примечания

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

2 Внутренний аудит проводит организация или внешняя сторона, привлекаемая организацией.

3.4

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

Примечания

1 Высшее руководство наделяет полномочиями и выделяет ресурсы внутри организации.

2 Если область применения системы управления 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, следует обеспечить координацию их деятельности.

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.1.23]

3.5

данные (data): Факты об объекте.
[ГОСТ Р ИСО 9000—2015, статья 3.8.1]

Примечание — В контексте систем управления ИТ-активами 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, предметы, процессы или идеи, включая концепции, которые в определенном контексте имеют конкретное значение, относящееся к ИТ-активам.

3.6 **документированная информация** (documented information): Информация, которую требуется использовать, хранить, контролировать с целью эффективного функционирования и развития организации, а также среда, в которой информация содержится.

Примечания

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

2 К документированной информации можно отнести:
- систему управления, включая связанные процессы;
- данные, используемые для надлежащего функционирования организации (документация);
- свидетельство, подтверждающее достижение поставленных целей (например, записи, ключевые показатели эффективности).

3.7 **достоверные данные** (trustworthy data): Данные и связанная с ними информация, проверенные уполномоченными лицами, отвечающими за их достоверность, которые однозначно истолкованы и доступны соответствующим пользователям на конкретный момент времени и достаточны для выполнения определенных задач.

Примечание — Определение термина «достоверные данные» изменено с целью формализации критериев отнесения к достоверным данным.

3.8

жизненный цикл (life cycle): Этапы, в течение которых осуществляется управление активом.

Примечание — Названия и количество этапов, а также видов деятельности на каждом этапе обычно специфичны для различных отраслей экономики и определяются организацией.

[ГОСТ Р 55.0.01—2014, статья 3.2.3]

Примечание — Основными этапами жизненного цикла ИТ-активов являются следующие: планирование, закупка, эксплуатация, выбытие ИТ-активов (см. приложение В).

3.9

заинтересованная сторона (stakeholder): Лицо или организация, которые могут воздействовать, или подвергаться воздействию, или считают, что может подвергаться воздействию решений или деятельности третьих лиц.

Примечание — Термин «Заинтересованная сторона» может также применяться как «вовлеченная сторона».

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.1.22]

3.10 **ИТ-актив** (IT asset): Оборудование, программное обеспечение, элемент или сущность, которые могут быть использованы для получения, обработки, хранения и распространения информации, способствовать предоставлению ИТ-продукта/услуги, а также имеет потенциальную или фактическую ценность для организации.

Примечания

1 ИТ-активы включают в себя:
- материальные (в т. ч. аппаратные) ИТ-активы;
- нематериальные (в т. ч. программные) ИТ-активы.

2 Услуги (сервисы), предоставляемые внешним поставщиком услуг, такие как программное обеспечение как услуга, облачные сервисы, техническое обслуживание оборудования, поддержка программного обеспечения, обучение и т. п., для отражения требований к управлению ИТ-активами также могут быть рассмотрены как ИТ-активы при соответствии их характеристик атрибутному составу, установленному внутри организации.

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

4 Информация сама по себе, независимо от материальных и нематериальных ИТ-активов, может считаться активом, но не ИТ-активом.

5 Связанный набор ИТ-активов также именуют ИТ-инфраструктурой.

6 Приведено общее определение термина ИТ-актив, включающее в себя как материальный, так и нематериальный ИТ-актив.

3.11 **измерение** (measurement): Процесс получения информации, совокупность действий для определения значений.

3.12 **ИТ-инфраструктур**а (IT infrastructure): Комплекс ИТ-активов для разработки, обслуживания, поддержки и использования ИТ-сервисов (услуг).

3.13

информация (information): Значимые данные.
[ГОСТ Р ИСО 9000—2015, статья 3.8.2]

Примечания

1 В контексте систем управления ИТ-активами 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). Данные могут относиться к таким объектам, как факты, события, предметы, процессы или идеи, включая понятия, которые в определенном контексте имеют определенное значение, связанное с ИТ-активами.

2 В контексте систем управления ИТ-активами информация может быть фиксирована в цифровом или бумажном виде.

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

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

3.15

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

[ГОСТ Р 55.0.01—2014, статья 3.1.8]

3.16 **компетенция** (competence): Наличие определенных знаний, умений и навыков, необходимых для осуществления определенной деятельности и достижения определенных результатов.

3.17

корректирующее действие (corrective action): Действие по устранению причины несоответствия и предотвращению его повторения.

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

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.4.1]

3.18

критический актив (critical asset): Актив, который может существенно повлиять на достижение целей организации.

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.2.7]

Примечания

1 Активы могут быть критическими для безопасности, для окружающей среды или для производительности и могут регулироваться законодательными и нормативными требованиями.

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

3.19 **материальный ИТ-актив** (hardware asset): Часть имущества организации, которая имеет материально-вещественную форму, является идентифицируемой частью ИТ-инфраструктуры, способной функционировать самостоятельно (не является неотделимой частью более крупного объекта), обладает стоимостной характеристикой, предназначенной для использования с целью предоставления ИТ-продукта/услуг и достижения целей организации, в т. ч. (но не ограничиваясь):

- устройства конечного пользователя;
- сетевое/коммутационное оборудование;
- оборудование центра обработки данных;
- периферийные устройства;
- мультимедиа (передача и преобразование видео-/аудиосигналов и сигналов управления, интерактивное, виртуальная реальность и пр.).

Примечание — Термин «аппаратное обеспечение» заменен на термин «материальный ИТ-актив» для приведения к единообразию перечня ИТ-активов, включенных в термин «ИТ-актив». Изменено определение термина с целью точного обозначения основных характеристик имущества организации, соответствующих критериям материального ИТ-актива.

3.20

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

Примечания

1 Для определения состояния может потребоваться проверка, надзор или наблюдение.

2 Для целей управления активами мониторинг может также относиться к определению состояния актива. Как правило, это относится к «мониторингу технического состояния» или «мониторингу производительности».

[ГОСТ Р 55.0.01—2014, статья 3.1.9]

3.21 **нематериальный ИТ-актив** (software IT): Часть имущества организации, которая не имеет материально-вещественной формы, является идентифицируемой единицей, предназначенной для ис-

пользования с целью предоставления ИТ-продукта/услуг и достижения целей организации, в том числе (но не ограничиваясь):

- программное обеспечение;
- лицензии (включая подтверждение лицензии);
- контракты;
- цифровой информационный актив (включая базы данных, базы знаний и прочие информационные ресурсы).

Примечания

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

2 Термин «программный актив» заменен на термин «нематериальный ИТ-актив» для приведения к единообразию перечня ИТ-активов, включенных в термин «ИТ-актив». Определение термина скорректировано для уточнения характеристик, признаков, которые относятся к нематериальным ИТ-активам.

3.22 **несоответствие** (nonconformity): Невыполнение требования.

3.23

постоянное улучшение (continual improvement): Повторяющаяся деятельность по улучшению производительности, базирующаяся на внутренних и внешних изменениях.

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.1.5]

3.24

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

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 комбинация перечисленного, объединение публичное или частное.

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.1.13]

3.25 **операционный план управления ИТ-активами** (IT asset management operational plan): Регламентированный порядок действий, необходимый для обеспечения непрерывной деятельности и поддержания актуальности данных по используемым ИТ-активам, соответствующих текущим задачам организации.

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

Примечания

1 Группировку активов можно производить по типу активов, системам активов или по портфелю ИТ-активов.

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

3 Данное определение является общим и может быть применено на всех уровнях планирования — от стратегического до операционного.

3.27 **портфель ИТ-активов** (IT asset portfolio): ИТ-активы, находящиеся в области применения системы управления ИТ-активами.

Примечания

1 Портфель ИТ-активов определяется и назначается для обеспечения аспектов управления активами соответствующего типа. Портфели для материальных ИТ-активов могут быть определены по категориям, например серверы, персональные компьютеры, мобильные устройства и т. д. Портфели программных ИТ-активов могут быть определены по производителю программного средства, по платформе, например персональные компьютеры, серверы, мейнфреймы, а также по области применения.

2 Система управления ИТ-активами может включать в себя несколько портфелей ИТ-активов.

3.28

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

[ГОСТ Р 55.0.01—2014, статья 3.1.15]

3.29

передать на аутсорсинг (outsource): Создать условия, когда внешняя организация выполняет часть функции или процессов организации.

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

[ГОСТ Р 55.0.01—2014, статья 3.1.16]

3.30

производительность (performance): Измеримый результат.

[ГОСТ Р 55.0.01—2014, статья 3.1.17]

Примечания

1 Производительность может относиться к количественным, так и к качественным параметрам оценки.

2 Производительность может относиться к управлению видами деятельности, процессами, продуктами (включая услуги), системами или организациями.

3 Для целей управления активами производительность может относиться к активам в части их способности выполнять требования или достигать целевых показателей.

3.31 **политика управления ИТ-активами** (IT asset management policy): Намерения, цели, принципы и курс организации, официально сформулированные и задокументированные ее высшим руководством в отношении управления ИТ-активами.

3.32

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

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

[ГОСТ Р 55.0.01—2014, статья 3.3.5]

3.33

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

Примечания

1 Это определение применимо только для деятельности по управлению активами.

2 Потенциальное несоответствие может иметь несколько причин.

3 Предупреждающее действие предпринимают для предотвращения возникновения несоответствия и сохранения функции актива, тогда как корректирующее действие 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.

[ГОСТ Р 55.0.01—2014, статья 3.3.4]

3.34

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

[ГОСТ Р 55.0.01—2014, статья 3.1.19]

3.35 **программное обеспечение** (software): Все программы или их часть, которые обрабатывают или поддерживают обработку цифровой информации.

Примечания

1 Для целей данного определения программное обеспечение исключает такую информацию, 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. Оно 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.

3.36

риск (risk): Следствие влияния неопределенности на достижение поставленных целей.
[ГОСТ Р ИСО 31000—2019, статья 3.1]

3.37 **санкция** (sanction): Мера, применяемая в случае нарушения требований, установленных внутренними нормативными документами организации, требований действующего законодательства или требований иных участников взаимоотношений.

3.38

система менеджмента (management system): Совокупность взаимосвязанных или взаимодействующих элементов организации для разработки политик, целей и процессов для достижения этих целей.
[ГОСТ Р 55.0.01—2014, статья 3.4.2]

Примечания

1 В контексте настоящего стандарта вместо термина «система менеджмента» используется термин «система управления».

2 Система управления может относиться к одной или нескольким областям.

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

4 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.

3.39 **система управления ИТ-активами;** ITAMS (IT asset management system, ITAMS): Система управления, обеспечивающая управление ИТ-активами, функции которой задают (определяют) политики и цели управления ИТ-активами организации.

Примечание — Система управления ИТ-активами является подмножеством управления активами.

3.40

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

Примечания

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

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

[ГОСТ Р 55.0.01—2014, статья 3.3.2]

Примечание — Стратегический план управления ИТ-активами разрабатывают на срок не менее 3 лет.

3.41

система активов (asset system): Совокупность активов, которые взаимодействуют или взаимосвязаны.

[ГОСТ Р 55.0.01—2014, статья 3.2.5]

3.42 **система ИТ-активов** (IT asset system): Набор ИТ-активов, которые взаимодействуют либо взаимосвязаны.

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

Примечание — Способности в рамках управления активами включают в себя процессы, ресурсы, компетенции и технологии, позволяющие эффективно и рационально разрабатывать и осуществлять планы по управлению активами, и процессы на всех этапах жизненного цикла актива, а также их постоянное улучшение.

3.44

соответствие (conformity): Выполнение требования.

[ГОСТ Р 55.0.01— 2014, статья 3.1.4]

3.45

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

Примечания

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

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

[ГОСТ Р 55.0.01—2014, статья 3.1.20]

3.46

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

Пример — Физические активы, информационные активы, нематериальные активы, критические активы, обеспечивающие активы, линейные активы, активы информационно-коммуникационных технологий, инфраструктурные активы, движимые активы.

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.2.6]

3.47

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

Примечания

1 В получение ценности обычно входит уравновешивание расходов, доходов, рисков, возможностей и производительности.

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

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

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.3.1]

3.48 **управление ИТ-активами;** ITAM (IT asset management, ITAM): Скоординированная деятельность организации по планированию, учету и отслеживанию ИТ-активов, обеспечивающая достижение целевых показателей для основной деятельности организации, предоставляющая прозрачный контроль финансовых потоков на протяжении жизненного цикла ИТ-активов с учетом внешних факторов

для принятия качественных управленческих решений о планировании, закупке, эксплуатации и выбытии ИТ-активов.

Примечание — Достижение целевых показателей для основной деятельности организации характеризуется ключевыми параметрами эффективности, безопасности, качества по этапам жизненного цикла ИТ-активов и определяется организацией.

3.49 **управление материальными ИТ-активами;** HAM (hardware IT asset management, HAM): Скоординированная деятельность организации по планированию, учету и отслеживанию материальных (в т. ч. аппаратных) ИТ-активов, являющихся идентифицируемой частью ИТ-инфраструктуры, которая обеспечивает достижение целевых показателей для основной деятельности организации и принятия качественных управленческих решений в процессе реализации учета, развертывания, обслуживания, контроля и мониторинга, обновления и выбытия материальных ИТ-активов организации.

Примечание — Управление материальными (в т. ч. аппаратными) ИТ-активами является специализированной частью процесса управления ИТ-активами, ориентированной на материально-вещественную ИТ-инфраструктуру.

3.50 **управление нематериальными ИТ-активами;** SAM (software IT asset management, SAM): Скоординированная деятельность организации по планированию, учету и отслеживанию нематериальных ИТ-активов (в т. ч. программных), обеспечивающая достижение целевых показателей для основной деятельности организации, выраженная в наборе ИТ-практик, процессов и технологий для управления и оптимизации использования нематериальных ИТ-активов в организации, их контроле и защите на всех этапах жизненного цикла, с целью принятия качественных управленческих решений о планировании, закупке, эксплуатации и выбытии нематериальных ИТ-активов.

Примечание — Термин «управление программными активами» переименован в термин «управление нематериальными ИТ-активами» с целью приведения к единообразию с видами ИТ-активов, входящими в определение термина «ИТ-актив».

3.51

уровень услуг (level of service): Параметры или сочетание параметров, которые отражают социальные, политические, природоохранные или экономические результаты деятельности организация.

[ГОСТ Р 55.0.01—2014, статья 3.3.6]

Примечания

1 В контексте настоящего стандарта вместо термина «уровень услуг» используется термин «уровень сервиса».

2 Параметрами уровня услуг могут быть следующие: безопасность, удовлетворенность клиента, качество, количество, объем, надежность, скорость реагирования, соответствие экологическим нормам, стоимость и доступность сервиса (услуг).

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

3.53

цель организации (organizational objective): Всеобъемлющая цель, в соответствии с которой устанавливают контекст и направление деятельности организации.

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

[Адаптировано из ГОСТ Р 55.0.01—2014, статья 3.1.14]

3.54 **цифровой актив** (digital asset): ИТ-актив, представленный в цифровом формате.

Примечание — Цифровые активы включают в себя программные активы и цифровые информационные активы.

3.55 **цифровой информационный актив** (digital information content asset): Актив в цифровом формате с информационным наполнением.

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

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

3.56

результативность (effectiveness): Степень реализации запланированных действий и достижения запланированных результатов.

[ГОСТ Р 55.0.01—2014, статья 3.1.7]

Примечание — В контексте настоящего стандарта вместо термина «результативность» используется термин «эффективность».

4 Контекст организации

4.1 Понимание организации и ее контекста

Организация должна определить внешние и внутренние задачи, которые имеют отношение к ее видам деятельности и влияют на способность организации достичь результатов в рамках системы управления ИТ-активами.

Примечание — Определение этих задач относится к установлению контекста организации, рассмотренного в ГОСТ Р ИСО 31000.

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 круг заинтересованных сторон, имеющих отношение к системе управления ИТ-активами;
- установить соответствующие требования и ожидания этих заинтересованных сторон в отношении управления ИТ-активами, а также требования с целью учета финансовых и нефинансовых данных, относящихся к управлению ИТ-активами, и для внутренней и внешней отчетности;
- определить критерии принятия решений по управлению ИТ-активами.

Примечание — В уточняющих целях добавлены новые критерии понимания потребностей и ожидания заинтересованных сторон.

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 задачи (см. 4.1);
- требования (см. 4.2);
- взаимодействие с другими системами управления в случае их использования.

Организация должна определить портфель(и) ИТ-активов, входящий(е) 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 и включать в себя:

- перечень ИТ-активов;
- системы и инструменты по управлению ИТ-активами;
- нормативно-правовую документацию по управлению ИТ-активами.

Примечание — Предметная область определяет, какие ИТ-активы включены в систему управления ИТ-активами.

4.4 Система управления ИТ-активами

Организация должна создавать, внедрять, 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, в котором будет представлена документация 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 собственные обязательства в отношении системы управления ИТ-активами посредством:

- определения и соответствия политики управления ИТ-активами, стратегического плана управления ИТ-активами и цели управления ИТ-активами стратегическим направлениям деятельности организации и организационным целям;
- определения способов интеграции требований системы управления ИТ-активами с требованиями бизнес-процессов организации;
- обеспечения доступности и достаточности ресурсов, необходимых для системы управления ИТ-активами;
- информирования о значимости эффективного управления ИТ-активами и обеспечения соответствия требованиям системы управления ИТ-активами;
- обеспечения достижения системой управления ИТ-активами намеченных результатов;
- направления и поддержки персонала во внесении собственного вклада в эффективность системы управления ИТ-активами (в том числе обучение, оценка, аттестация и сертификация персонала);
- содействия кросс-функциональному сотрудничеству внутри организации;
- содействия постоянному улучшению процессов;
- демонстрации приоритетности других соответствующих управленческих ролей применительно к их зонам ответственности;
- обеспечения согласованности подхода к управлению рисками при управлении ИТ-активами с общим подходом к управлению рисками в организации;
- обеспечения документирования и стандартизации процессов по управлению ИТ-активами.

Примечания

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

2 По тексту подраздела в качестве уточнения добавлены следующие фразы: «достаточности», «персонала», «в т. ч. обучение и сертификация персонала», «обеспечения документирования и стандартизации процессов по управлению ИТ-активами».

5.2 Политика

Политика управления ИТ-активами определяет единый подход в области управления ИТ-активами (курс, цели, принципы и намерения, заинтересованные стороны и т. д.).

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

а) соответствует целям организации;

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

в) включает обязательства соблюдения установленных требований организации и постоянного совершенствования системы управления ИТ-активами.

5.2.2 Политика управления ИТ-активами должна:

а) соответствовать организационному плану;

б) не противоречить иным политикам организации, включая политики других систем управления, используемых организацией, а также соответствующим стратегическим планам других систем управления, используемых организацией;

в) соответствовать характеру и масштабу ИТ-активов организации и связанной с ними операционной деятельности;

г) соответствовать обязательствам отдельных лиц и организации по контролю за ИТ-активами;

д) определять критерии эффективного использования ИТ-активов для нужд и задач организации;

е) обеспечивать исполнение политики организации в отношении условий контрактов, связанных с ИТ-активами, включая требования лицензионных соглашений (лицензирования) ПО;

ж) быть доступной для всех сотрудников организации, в т. ч. для заинтересованных сторон (в зависимости от степени вовлеченности);

и) включать в себя описание санкций за нарушение данной политики;

к) исполняться, периодически пересматриваться и при необходимости обновляться.

5.3 Роли в организации, ответственности и полномочия

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

5.3.2 Высшее руководство должно устанавливать уровень ответственности и определять соответствующие полномочия:

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

б) для соблюдения поддержки системой управления ИТ-активами реализации стратегического плана управления ИТ-активами;

в) для гарантии соответствия системы управления ИТ-активами требованиям настоящего стандарта;

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

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

е) для предоставления отчетности по эффективности системы управления ИТ-активами для высшего руководства;

ж) для обеспечения соблюдения и контроля за выполнением политики управления ИТ-активами со стороны всех сотрудников организации (включая санкции за несоблюдение);

и) для предоставления своевременного информирования об изменении положений в политике управления ИТ-активами.

6 Планирование

6.1 Виды планирования

В рамках управления ИТ-активами выделяют:

- стратегическое планирование (см. 6.1.1);
- операционное планирование (см. 6.1.2).

6.1.1 Общие положения по стратегическому планированию управления ИТ-активов

При стратегическом планировании в управлении ИТ-активами организация должна учитывать задачи, указанные в 4.1, и требования, перечисленные в 4.2, определять те риски и возможности, которые необходимо учитывать:

- для того чтобы система управления ИТ-активами могла способствовать достижению запланированных результатов;
- предотвращения или уменьшения нежелательных последствий;
- достижения постоянного улучшения.

Организация должна сформулировать:

а) долгосрочную стратегию управления ИТ-активами, которая включает в себя:

1) цели и задачи по управлению ИТ-активами,

2) план автоматизации и/или оптимизации существующих процессов,

3) действия по устранению рисков с учетом возможности их изменения во времени;

б) дорожную карту по достижению целей стратегии;

в) критерии эффективности управления ИТ-активами.

6.1.2 Общие положения по операционному планированию управления ИТ-активами

При операционном планировании в управлении ИТ-активами организация должна:

а) сформировать план по объемам ИТ-активов, требуемых для обеспечения технологической устойчивости организации;

б) сформировать план распределения ИТ-активов в соответствии с потребностью организации;

в) сформировать график контрольных мероприятий, в том числе:

1) проведение сверок,

2) проведение инвентаризаций,

3) подготовка отчетности для аудиторов,

4) корректировка данных об ИТ-активах в системах учета ИТ-активов;

г) сформулировать план выбытия ИТ-активов;

д) сформулировать критерии эффективности процедур по операционному управлению ИТ-активами.

Примечание — Существуют значительные различия между операционным и стратегическим планированием в рамках управления ИТ-активами. Для повышения эффективности управления планирование разделено на стратегическое и операционное с формализацией основных критериев по каждому виду планирования.

6.1.3 Оценка рисков ИТ-активов

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

а) устанавливает и поддерживает критерии риска ИТ-активов, включающие критерии:

1) принятия риска,

2) выполнения оценки рисков ИТ-активов;

б) обеспечивает получение согласованных, действительных и сопоставимых результатов при повторных оценках рисков ИТ-активов;

в) идентифицирует риски ИТ-активов:

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

- риски, связанные с потерей конфиденциальности, целостности и доступности для ИТ-активов, входящих в состав системы управления ИТ-активами,
- риски непрерывности бизнеса,
- риски несоответствия правовым и нормативным требованиям,
- риски, связанные с соблюдением договорных обязательств, включая риск несоответствия лицензионным соглашениям,

2) определяет владельцев риска.

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

г) анализирует риски ИТ-активов:

1) оценивает потенциальные последствия, которые могут возникнуть, если риски, идентифицированные в 6.1.3, перечисление в) 1), материализовались,

2) оценивает реальную вероятность возникновения идентифицируемых рисков в 6.1.3, перечисление в) 1),

3) определяет уровни риска;

д) оценивает риски ИТ-активов:

1) сравнивает результаты анализа рисков с критериями риска, установленными в 6.1.2, перечисление а),

2) определяет приоритет проанализированных рисков для обработки рисков.

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

6.1.4 Реакция на риски для ИТ-активов

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

а) принять надлежащие меры по снижению рисков ИТ-активов с учетом результатов оценки рисков и возможных ограничений по использованию.

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

б) установить перечень всех контрольных мероприятий, необходимых для реализации выбранного(ых) варианта(ов) обработки рисков ИТ-активов.

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

в) сформулировать план обработки рисков ИТ-активов;

г) согласовать с высшим руководством план обработки рисков ИТ-активов и 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 ГОСТ Р ИСО 31000, а также с требованиями, указанными в ГОСТ Р ИСО/МЭК 27001—2021 (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 в отношении управления ИТ-активами.

Примечания

1 В приложении В приведен перечень рабочих процессов для управления ИТ-активами, который не является исчерпывающим, поэтому может потребоваться использование дополнительных рабочих процессов.

2 Возможно, но необязательно указывать группы процессов для включения или исключения на основе их распределения по уровням (см. приложение Б).

6.2.2 Цели управления ИТ-активами для операционных процессов

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

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

Примечания

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

2 Термин «положение о применимости» выбран по аналогии со способами и принципами применимости, описанными в ГОСТ Р ИСО/МЭК 27001. Положение о применимости совместно с определением предметной области (4.3) необходимо внутренней или внешней стороне для определения того, что включает в себя система управления ИТ-активами.

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

6.2.3 Общие цели управления ИТ-активами

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

Цели управления ИТ-активами должны обеспечивать достижение основополагающих показателей для основной деятельности организации, предоставляющей прозрачный контроль финансовых потоков на протяжении жизненного цикла ИТ-активов с учетом всех факторов для принятия качественных и своевременных управленческих решений о планировании, закупке, эксплуатации и выбытии ИТ-активов.

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 должны:

- 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;
- содержать количественные целевые показатели для обеспечения точности данных;
- учитывать применимые требования;
- отражать (по мере возможности) вероятность высоких темпов изменений в технологии и в бизнес-окружении;
- быть контролируемыми;
- быть доступными для всех сотрудников организации, в том числе для заинтересованных сторон (в зависимости от степени вовлеченности);
- пересматриваться и обновляться в соответствии с обстоятельствами.

3 В уточняющих целях сформулированы требования к целям управления ИТ-активами.

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

6.2.4 Планирование достижения целей управления ИТ-активами

Организации необходимо синхронизировать 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 должен(ы) соответствовать политике управления ИТ-активами и стратегическому плану управления ИТ-активами.

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

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

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

б) процессы и методы, которые должны быть использованы для управления ИТ-активами в течение их жизненных циклов;

в) метрики соответствия достижения плановых показателей, в том числе:

1) ресурсы для достижения показателей,

2) ответственные на всех этапах процесса управления жизненным циклом ИТ-активов,

3) сроки достижения плановых показателей;

г) финансовые и нефинансовые результаты плана(ов) управления ИТ-активами;

д) периодичность пересмотра планов управления ИТ-активами.

7 Поддержка

7.1 Ресурсы

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

Организация должна обеспечить ресурсы, необходимые для достижения целей управления ИТ-активами и для осуществления действий, определенных в планах управления ИТ-активами.

7.2 Компетенции

Организация должна:

- определять необходимые компетенции лиц(а), осуществляющих(его) деятельность под контролем организации, которая влияет на эффективность использования ИТ-активов, управления ИТ-активами и системы управления ИТ-активами;
- гарантировать, что лица, занятые в управлении ИТ-активами и поддержке систем управления ИТ-активами, компетентны на основании соответствующего образования, периодического обучения или фактического опыта;
- при возможности, принимать меры для приобретения необходимой компетенции и оценивать эффективность принятых мер;
- сохранять соответствующую документированную информацию как доказательство компетенции;
- периодически пересматривать текущие и потенциальные потребности и требования к компетенциям.

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

7.3 Осведомленность

Лица, которые осуществляют деятельность под контролем организации и которые могут оказывать влияние на достижение целей управления ИТ-активами, должны быть осведомлены:

- о политике управления ИТ-активами (см. 5.2), в том числе об ответственности за несоблюдение требований политики управления ИТ-активами;
- стратегии управления ИТ-активами;
- целях в управлении ИТ-активами;
- об операционном плане управления ИТ-активами (см. 6.1);
- о стратегическом плане управления ИТ-активами (см. 6.1);
- об их вкладе в эффективность системы управления ИТ-активами, включая выгоды от повышения эффективности управления ИТ-активами;
- их трудовой деятельности, сопутствующих рисках и возможностях и о том, как они взаимосвязаны друг с другом;
- о последствиях отклонений (санкциях) от требований системы управления ИТ-активами.

7.4 Коммуникация

Организация должна определить потребность во внутренних/внешних коммуникациях и порядок взаимодействия лиц, имеющих отношение к ИТ-активам, управлению ИТ-активами и системе управления ИТ-активами.

7.5 Информационные требования

Организация должна определить свои информационные требования для поддержки ее ИТ-активов, управления ИТ-активами, системы управления ИТ-активами и для достижения ее целей в управлении ИТ-активами, а также целей организации. Требования могут включать, но не ограничиваться финансовой, закупочной, договорной, лицензионной, технической информацией и информацией об организации. При этом организация должна:

а) принять во внимание:

1) значимость выявленных рисков,

2) сложность контроля характеристик ИТ-активов (см. приложение В),

3) роли и ответственность в управлении ИТ-активами,

4) какие метрики необходимы для определения целевых показателей организации в управлении ИТ-активами,

5) процессы, процедуры и действия по управлению ИТ-активами,

6) обмен информацией с заинтересованными сторонами, включая поставщиков товаров и услуг,

7) воздействие качества, доступности и управления информацией на принятие организационных решений,

8) требования законодательства к учету и использованию ИТ-активов;

б) определить:

- требования к атрибутам идентифицированной информации,
- требования к качеству идентифицированной информации,
- как и когда информация должна собираться, анализироваться и оцениваться;

в) определить, внедрить и поддерживать процессы управления атрибутами и данными об ИТ-активах организации;

г) определить требования для согласования финансовой и нефинансовой терминологии, относящейся к управлению ИТ-активами повсеместно в организации;

д) гарантировать согласованность и прослеживаемость между финансовыми, техническими данными, а также другими нефинансовыми данными об ИТ-активах в объеме, необходимом для ее соответствия законодательству, с учетом нормативных документов и требований заинтересованных сторон, а также целей организации.

7.6 Документированная информация

7.6.1 Общие положения

Система управления ИТ-активами организации должна включать документированную информацию:

- в соответствии с требованиями настоящего стандарта;
- согласно требованиям действующего законодательства;
- определенную организацией как необходимую для управления ИТ-активами в соответствии с 7.5.

Примечания

1 Объем документированной информации для системы управления ИТ-активами в организациях может отличаться в связи:

- с размером организации и ее видом деятельности, процессами, продуктами и услугами;
- со сложностью процессов и их взаимодействием;
- с компетентностью персонала;
- со сложностью и количеством ИТ-актива(ов);
- с уровнем зрелости организации.

2 Информационные требования по 7.5 касаются определения общих требований ИТ-системы, что является первоначальной задачей, связанной с разработкой системы управления ИТ-активами, однако требования следует периодически пересматривать. В 7.6 рассмотрена такая информация в целях владения проверяемой информацией, т. е. контрольного следа.

7.6.2 Прослеживаемость владения и ответственности

Владение и ответственность за все ИТ-активы должны быть подтверждены документированной информацией, соответствующей требованиям действующего законодательства и определенной как необходимая и достаточная.

Примечания

1 Документация по владению и ответственности может иметь любой уровень детализации или обобщенности, который организация считает соответствующим. При применении смешанных способов владения и ответственности как для устройств конечного пользователя и серверов, так и для ПО 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 за собой ответственность за другой тип ИТ-актива. Например, изменение конфигурации оборудования или перемещение оборудования в некоторых случаях может стать причиной изменения лицензионной составляющей.

7.6.3 Контрольный след авторизаций и выполнение авторизаций

Все доступы к информации об ИТ-активах и к системе управления ИТ-активами должны быть документально подтверждены. Документированная информация должна включать подробную информацию о том:

а) кто согласовал авторизацию и доступ;

б) когда предоставлены авторизация и доступ;

в) на какой срок предоставлены авторизация и доступ;

г) что является основанием предоставления авторизации и доступа.

Примечания

1 Не требуется наличия каких-либо конкретных типов авторизаций, если иное не определено в настоящем стандарте и/или требованиях организации. 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 типам ИТ-активов. Авторизации также могут быть ограничены во времени. Кроме того, могут существовать различные уровни авторизаций, такие как финансовые, безопасности, оперативные и управленческие.

2 Примером выполнения авторизаций является установка авторизованного (или с полномочиями на изменение) ПО или получение доступа к системе.

3 Документированной информацией в данном случае может являться согласование ответственными лицами предоставления доступа в электронном виде и/или через систему получения доступов организации.

7.6.4 Создание и изменение

При создании и обновлении документированной информации организация должна обеспечить:

- качественную идентификацию и описание информации (например, наименование, дата, автор или ссылочный номер);
- надлежащий формат (например, язык, версия ПО, графика) и носители (например, бумажные, электронные);
- надлежащую оценку и утверждение актуальности информации.

7.6.5 Контроль документированной информации

Документированная информация, касающаяся системы управления ИТ-активами и положений настоящего стандарта, должна контролироваться и быть:

а) доступной для всех сотрудников организации, в том числе для заинтересованных сторон (в зависимости от степени вовлеченности);

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

Организация обязана осуществлять контроль за документированной информацией в соответствии с действующим законодательством и обеспечивать контроль:

- за распространением, доступом, извлечением и использованием;
- хранением и защитой, включая сохранение разборчивости и целостности;
- изменениями (например, контроль версий);
- сохранностью и размещением.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и эксплуатации ИТ-активов и 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

Все операционные процессы управления ИТ-активами в организации делятся в соответствии с этапами жизненного цикла ИТ-активов (например, планирование, поставка, эксплуатация, выбытие).

8.1 Операционный контроль

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

- определения критериев контроля процессов;
- осуществления контроля процессов в соответствии с критериями;
- хранения документированной информации в объеме, необходимом для подтверждения того, что процессы выполняются в соответствии с планом;
- обработки и мониторинга 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 по таким основным критериям, как:

- импортонезависимость (импортозамещение);
- непрерывность деятельности;
- информационная безопасность;
- безопасность условий труда;
- соблюдение авторских прав;
- производительность.

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.

Примечание — Добавлены новые критерии в связи с появлением новых ограничений и изменением технической политики в Российской Федерации.

8.3 Управление основными данными об ИТ-активах

Организация должна обеспечить, чтобы необходимые данные обо всех основных ИТ-активах точно регистрировались и поддерживались в актуальном состоянии на протяжении всего жизненного цикла и чтобы по всем ИТ-активам была доступной документированная информация по ключевым атрибутам ИТ-активов.

Организация должна обеспечить, чтобы необходимые данные и информация о нематериальных ИТ-активах, о связанных правах и использовании в соответствии с правами для всех ИТ-активов в процессе были точно зарегистрированы в течение жизненного цикла ИТ-актива, а также нести ответственность за периодическое проведение аудита, оценки и верификации соответствующих требований.

Примечания

1 Основные ИТ-активы включают в себя материальные и нематериальные ИТ-активы. Цифровые информационные активы (например, лицензированные аудио- и видеозаписи, текстовые и PDF-документы) также считают нематериальными ИТ-активами, если они включены в процесс. В ситуациях со смешанной ответственностью (например, для облачных вычислений или BYOD) может быть целесообразным включить ИТ-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 Данный процесс предоставляет информацию об ИТ-активах для поддержки эффективности и результативности других бизнес-процессов.

4 Примером атрибутного состава, отвечающего требованиям по полноте данных материальных ИТ-активов, может являться следующая структура:

- наименование ИТ-актива;
- изготовитель/поставщик;
- тип/категория ИТ-актива;
- серийный номер;
- пользователь/ответственное лицо;
- собственник;
- статус (меняется в соответствии с жизненным циклом организации, например поступил, в эксплуатации, списан и пр.);
- стоимость ИТ-актива;
- местоположение ИТ-актива.

5 Примером атрибутного состава, отвечающего требованиям по полноте данных нематериальных ИТ-активов, может являться следующий состав:

- статус (меняется в соответствии с жизненным циклом организации, например поступил, в эксплуатации, списан и пр.);
- тип/категория ИТ-актива;
- изготовитель;
- поставщик;
- собственник;
- наименование;
- стоимость;
- количество;
- дата начала действия;
- дата окончания действия;
- сведения о технической поддержке;
- сведения о метрике лицензирования.

6 Если цифровые информационные активы включены в процесс и на них распространяются условия лицензирования, на них также будут распространены эти требования.

7 Каждая организация в зависимости от своих целей и потребностей в части обеспечения качества данных, осуществления контроля и мониторинга ИТ-активов уточняет/дополняет обязательный атрибутный состав. В целях стандартизации типовых операций в организации должен быть утвержден перечень атрибутов и определены правила их заполнения.

8.4 Управление безопасностью

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

- информационной безопасности;
- безопасности условий труда.

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

8.5 Другие процессы

Организация должна обеспечить функционирование других процессов (см. 6.2.2), а также дополнительных процессов, определенных организацией.

Примечание — Этот подраздел является механизмом добавления дополнительных процессов, как определено в приложениях Б, В.

8.6 Аутсорсинг и услуги

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

Примечания

1 Аутсорсинговая деятельность включает в себя услуги, предоставляемые извне. Примерами подобного рода услуг являются следующие: ПО как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS), а также техническое обслуживание оборудования, поддержка ПО и обучение. Однако термин «аутсорсинг», как правило, используется с относительно всеобъемлющим набором услуг, в то время как отдельные услуги, как правило, считаются более ограниченными по области применения.

2 Дополнительная информация об управлении аутсорсингом и услугами приведена в ГОСТ Р 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, она 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), серверами (организация и третья сторона, например для облачных вычислений), лицензируемым ПО (принадлежащим организации или третьей стороне), а также хранимыми и обрабатываемыми данными (организации, персонала или третьей стороны).

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

Организация должна определить:

а) 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);

б) последствия при наличии смешанной ответственности (включая связанные с этим риски и то, как совместная ответственность может быть эффективно реализована с помощью подотчетности ответственных лиц);

в) ответственность и полномочия в организации по управлению внешними процессами и деятельностью, в том числе юридические аспекты применения аутсорсинговых процессов;

г) процессы, инструменты, порядок и возможности для обмена знаниями и информацией между организацией и ее поставщиком(ами) услуг по контрактам;

д) механизм контроля процессов, переданных на аутсорсинг;

е) последовательность, форму и критерии оценки качества выполнения процессов, переданных на аутсорсинг.

При аутсорсинге любой деятельности организация должна обеспечить, чтобы:

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

8.7 Смешанная ответственность организации и ее персонала

Когда организация и ее персонал несут смешанную ответственность за ИТ-активы (с учетом 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 подобных ситуаций.

Примечания

1 Ситуации, связанные со смешанной ответственностью между организацией и ее персоналом, включают в себя практику использования собственного устройства (BYOD) для деятельности организации, а также ИТ-активов организации в личных целях как результат хранения личных данных или информации на ресурсах организации. Когда организация применяет ИТ-инфраструктуру со смешанной ответственностью за ИТ-активы, или данные, или информацию между организацией и ее персоналом, она должна оценить связанные с этим риски. Организация также должна обеспечить контроль процессов и ИТ-инфраструктуры, связанных с такой смешанной ответственностью.

2 Примером ситуации, связанной со смешанной ответственностью, является ответственность разных участников за использование устройств конечного пользователя (корпоративные, или личные, или принадлежащие третьей стороне, такой как оператор мобильной связи), лицензируемого ПО (корпоративного, личного или ПО третьей стороны), данных и информации, которые хранят и обрабатывают в организации (корпоративно, лично или третьей стороной).

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

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

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

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

г) 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 соответствовали 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

9.1.1 Организация может распределить ИТ-активы по степени критичности следующим образом:

а) критические. Потенциальный ущерб предельно высокий. Потеря доступности, конфиденциальности и/или целостности оказывает тяжелое или катастрофически вредоносное воздействие на деятельность организации, ее активы и персонал, т. е. организация теряет способность выполнять все или некоторые из своих основных функций, активам причиняется крупный ущерб, организация несет крупные финансовые и репутационные потери, персоналу наносится тяжелый или катастрофический вред, создающий возможную угрозу жизни или здоровью;

б) важные. Потенциальный ущерб высокий или средний. Потеря доступности, конфиденциальности и/или целостности оказывает существенное вредоносное воздействие на деятельность организации, ее активы и персонал: организация остается способной выполнять возложенную на нее миссию, но эффективность основных функций оказывается значительно сниженной, активам причиняется значительный ущерб, организация несет значительные финансовые и репутационные потери, персоналу наносится значительный вред, не создающий угрозы жизни или здоровью;

в) поддерживающие. Потенциальный ущерб низкий или предельно низкий. Потеря доступности, конфиденциальности и/или целостности не оказывает или оказывает ограниченное негативное воздействие на деятельность организации, ее активы и персонал: организация остается способной выполнять возложенную на нее миссию, эффективность основных функций оказывается сниженной, активам при-

чиняется незначительный ущерб, организация несет незначительные финансовые потери, персоналу наносится незначительный вред.

Примечание — Степени критичности выделены для совершенствования системы управления ИТ-активами, которая существенно влияет на параметры мониторинга, аудита и т. п.

9.1.2 При распределении по степени критичности организация определяет:

а) каким категориям ИТ-активов необходимы мониторинг и измерения;

б) виды мониторинга, измерения, анализа и оценки, которые применимы для обеспечения достоверных результатов. Выделяют следующие виды мониторинга и аудита:

1) фактический мониторинг: физическая проверка состояния и статуса ИТ-актива по месту его нахождения,

2) удаленный мониторинг: проверка состояния и статуса ИТ-актива в режиме реального времени с помощью специализированных систем мониторинга,

3) сверка данных систем: сверка соответствующих атрибутов различных систем учета ИТ-активов (система оперативного, бухгалтерского учета, удаленного мониторинга), выявление расхождений/соответствий с целью повышения качества данных;

в) периодичность выполнения мониторинга и измерения;

г) порядок выполнения мониторинга и измерения;

д) порядок, сроки, критерии формирования, оценки и анализа результатов измерения и мониторинга.

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

Примечание — С целью выбора наиболее подходящего способа проведения организацией мониторинга ИТ-активов даны определения видам мониторинга и уточнены параметры.

9.1.3 Организация должна оценивать эффективность:

- использования ИТ-активов;
- управления ИТ-активами, включая финансовые и нефинансовые показатели;
- системы управления ИТ-активами;
- процессов управления рисками и возможностями.

Организация должна обеспечить проведение мониторинга и выполнение измерений, позволяющих соответствовать требованиям 4.2.

9.2 Внутренний аудит

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

а) соответствует:

1) собственным требованиям организации к системе управления ИТ-активами,

2) целям организации,

3) целям управления ИТ-активами,

4) требованиям настоящего стандарта;

б) внедрена, эксплуатируется и поддерживается.

9.2.2 Организация должна:

а) запланировать, утверждать, реализовывать и поддерживать план проведения аудита, включающий требования к частоте, методам, ответственности, планированию и отчетности, который должен учитывать значимость соответствующих процессов и результаты предыдущих аудитов;

б) определять критерии и масштаб для каждого аудита;

в) осуществлять надлежащий подбор аудиторов и проводить аудиты в соответствии с требованием об обеспечении объективности и беспристрастности процесса аудита;

г) обеспечивать, чтобы результаты проведенных аудитов были представлены к рассмотрению ответственным лицам;

д) осуществлять хранение документированной информации по проведенным аудитам в качестве доказательства реализации программы аудита и результатов аудита.

9.3 Управленческий контроль

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

Управленческий контроль должен учитывать:

а) динамику основных показателей из предыдущих управленческих контролей;

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

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

1) о выявленных несоответствиях данных в системе управления ИТ-активами,

2) корректирующих действиях,

3) результатах мониторинга и измерений,

4) результатах аудита;

г) процессы управления ИТ-активами;

д) возможности для непрерывного улучшения;

е) изменения в профиле рисков и возможностей.

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

Организация должна хранить документированную информацию в качестве свидетельства результата проведения управленческого контроля.

10 Улучшение

10.1 Несоответствие и корректирующее действие

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

а) задокументировать обстоятельства несоответствия и/или инцидента;

б) реагировать надлежащим образом на несоответствие и/или инцидент, а именно:

1) принять меры для контроля и исправления выявленных несоответствий,

2) разработать критерии эффективности корректирующих действий по инцидентам и/или несоответствиям;

в) оценить необходимость действия по устранению причин(ы) несоответствия и/или инцидента, чтобы они не повторялись или не происходили в другом месте, путем:

1) рассмотрения несоответствия и/или инцидента,

2) выяснения причин несоответствия и/или инцидента,

3) определения возможности возникновения несоответствий и/или инцидентов в дальнейшем;

г) проверить эффективность любых предпринятых корректирующих действий;

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

Корректирующие действия должны быть соразмерны последствиям произошедших выявленных несоответствий и/или инцидентов.

Организация должна хранить документированную информацию в качестве свидетельства:

- причин происхождения несоответствий и/или инцидента;
- последующих предпринятых действий;
- результатов и эффективности любых корректирующих действий.

10.2 Профилактические действия

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

Для этого организация должна:

а) фиксировать все инциденты с ИТ-активами;

б) систематизировать и анализировать причины возникновения инцидентов с ИТ-активами;

в) организовать процесс отработки и внедрения корректирующих действий по процессам управления ИТ-активами;

г) назначить ответственного, определить сроки исполнения и внедрения корректирующих действий по процессам управления ИТ-активами;

д) анализировать результаты корректирующих действий за отчетный период.

При выявлении потенциального сбоя организация должна соблюдать требования 10.1.

10.3 Непрерывное улучшение

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

а) стратегического планирования управления ИТ-активами;

б) операционного планирования управления ИТ-активами;

в) годового планирования управления ИТ-активами;

г) оценки эффективности использования ИТ-активов, управления ИТ-активами, системы управления ИТ-активами;

д) проведения внутреннего аудита;

е) оценки зрелости систем и процессов управления ИТ-активами.

Приложение А
(справочное)

Характеристики нематериальных ИТ-активов

А.1 Данное приложение содержит обзор характеристик ИТ-активов, которые создают дополнительные или более детальные требования, предъявляемые к системе управления ИТ-активами (ITAMS) по сравнению с аналогичной для физических активов, не относящихся к ИТ-активам, а также те положения, которые необходимо учитывать при определении информационных требований для ITAMS (см. введение и 7.5).

А.2 Сущность ПО

Программное обеспечение является одним из наиболее значимых активов, которыми необходимо управлять в рамках управления ИТ-активами (ITAM), и обладает рядом характеристик, которые создают следующие требования к управлению:

а) простота изменения, копирования и распространения ПО. Поскольку ПО является электронным, а не физическим (в общепринятом смысле), оно может быть изменено, скопировано и распространено. Это создает значительные риски для несанкционированных (вредоносных или невредоносных) изменений и использования ПО;

б) технологическая сложность. Программные активы, как правило, сложнее физических активов во многих аспектах, таких как:

1) гибкость размещения. ПО может быть сохранено или установлено в одном месте, но может быть задействовано или применено с учетом дополнительных экземпляров или мест размещения, например ПО с использованием виртуальных машин или предназначенное для облачных сервисов, ПО как услуга (SaaS), платформа как услуга (PaaS) и инфраструктура как услуга (IaaS), а также посредством сетевого доступа к ПО, размещенному на сервере,

2) количество и сложность компонентов. Как правило, ПО содержит больше компонентов, чем физические активы, например: на типичном персональном компьютере могут находиться сотни тысяч файлов, а отдельные компоненты могут быть предельно сложны,

3) темпы изменений. Обычно темпы изменений ПО высокие, намного превышающие темпы изменения физических активов,

4) версии компонентов. Существуют жесткие требования к версионности программных компонентов, которые следует контролировать для достижения многих целей, в том числе для обеспечения безопасности, совместимости и лицензирования,

5) анализ использования. Часто сложно провести объективный анализ использования ИТ-активов, особенно ПО, который может потребоваться как в целях общего управления, так и для соблюдения контрактных обязательств. Анализ использования ПО может также зависеть от применяемого оборудования и проведения прочих измерений, например: от процессоров или ядер, от количества пользователей, устройств, инсталляций и т. п.;

в) лицензирование. Управление лицензированием и соблюдение условий лицензирования является основным требованием для управления ПО, которое не применяется к физическим активам. Как правило, ПО — это сложный объект лицензирования. Каждый правообладатель (производитель) самостоятельно устанавливает условия использования ПО, включая возможные ограничения. Более того, условия лицензирования часто меняются в рамках не только отрасли или конкретных производителей, но и отдельных продуктов и версий продуктов конкретных производителей;

г) нечеткое различие между программным и аппаратным обеспечением. Физические активы, в том числе ИТ-оборудование, все чаще имеют существенные программные компоненты, которые часто сложны при управлении ПО даже в контекстах, типично рассматривающихся как чисто физические, например:

1) встроенное ПО. Физические активы все чаще имеют встроенное ПО для контроля и/или мониторинга,

2) программная реализация аппаратных функций. Функциональность оборудования, как правило, является частью ПО, например: в платформах виртуализации и эмуляции, а также в программно-определяемых сетях,

3) носитель. Носитель — это термин, который применяется как к физическим, так и к программным активам, причем оба типа требуют управления;

д) повышенное внимание к выводу из эксплуатации/переназначению. При выводе из эксплуатации/переназначении ИТ-активов необходимо руководствоваться более жесткими требованиями, чем предъявляемые к физическим активам. Это связано с необходимостью защиты данных, информации, а также защитой от других возможных воздействий на данном этапе жизненного цикла ИТ-активов, в основном это касается:

1) ПО, данных и информации. Следует контролировать ПО, данные и информацию ИТ-активов при выводе из эксплуатации/переназначении оборудования, например во избежание раскрытия конфиденциальной и личной информации, а также с учетом задач соответствия, связанных с ПО,

2) электронных отходов. В большинстве юрисдикций существуют жесткие требования к контролю за удалением электронных отходов, вплоть до того, что они должны рассматриваться как общие требования к управлению ИТ-активами;

е) повышенные сложности управления. Существует ряд сложностей, характерных для управления ИТ-активами, которые требуют особого внимания в отношении их управления, в частности:

1) смешанное владение/ответственность. В настоящее время для ИТ-активов типично использование в смешанном режиме владения. Например, стороны могут владеть устройствами, применяемыми конечными пользователями (организация, или частные лица, или даже третья сторона), серверами (организация или третья сторона для случая облачных вычислений), ПО (организация, частные лица, третья сторона), а также данными и информацией, которые хранят и обрабатывают (организация, частные лица или третья сторона),

2) отсутствие взаимодействия между системами управления ИТ-активами и финансовыми системами. Ввиду сравнительно низких затрат на большинство ИТ-активов они обычно относятся к расходам, а не капитализируются, что приводит к существенным сложностям для сверки данных об ИТ-активах между системами управления ИТ-активами и финансовыми системами. Если эти системы не могут быть синхронизированы, это может вызвать вопросы к системе управления ИТ-активами относительно объективного положения дел со стороны финансового и управленческого персонала,

3) расхождения между технологическим обеспечением и договорными условиями. Ввиду быстро развивающихся технологических возможностей часто возникают расхождения между фактическим использованием ИТ-активов и условиями контрактов, регулирующих их применение, которые, как правило, отстают от применяемых технологий.

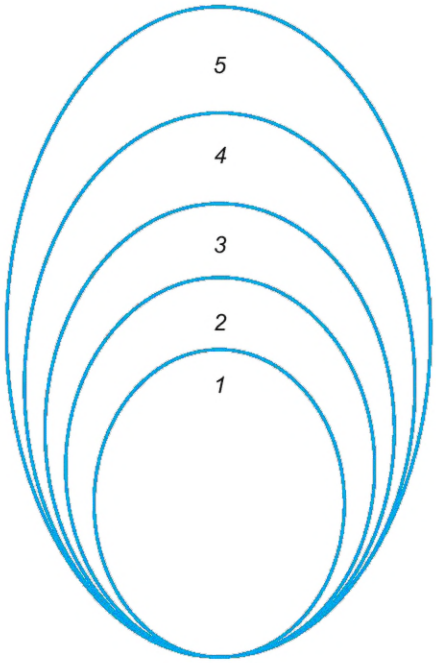
Приложение Б
(справочное)

Уровни зрелости управления ИТ-активами

В данном приложении представлено описание уровней зрелости, определенных для их дополнительного использования с учетом требований настоящего стандарта.

Уровни зрелости — этапы развития процессов организации в соответствии со стандартизованной моделью, происходящие последовательно и определяемые различными характеристиками, включающими специфику, политику, стратегию, систему управления ИТ-активами, организационную структуру и т. д.

Уровни зрелости показаны на рисунке Б.1.



1 — осуществляемый; *2* — управляемый; *3* — установленный; *4* — предсказуемый; *5* — оптимизирующий

Рисунок Б.1 — Уровни зрелости управления ИТ-активами

Предполагается, что уровни зрелости должны иметь нарастающий характер, т. е. организация, которая хочет соответствовать требованиям уровня 2, также должна соответствовать требованиям уровня 1, и аналогично — организация, которая хочет соответствовать требованиям уровня 5, также должна соответствовать требованиям уровней 1, 2, 3 и 4.

Таблица Б.1 — Уровни зрелости управления ИТ-активами

Уровень зрелости	Определение уровня зрелости
Уровень 1 «Осуществленный»	Осуществленный процесс достиг своего назначения. Организация понимает, какими ИТ-активами обладает и может ими управлять
Уровень 2 «Управляемый»	Описанный выше осуществленный процесс на данном уровне выполняют управляемым образом (планируют, регулируют и проводится его мониторинг), а его рабочие продукты соответствующим образом установлены, контролируются и поддерживаются на протяжении всего жизненного цикла ИТ-актива
Уровень 3 «Установленный»	Описанный выше управляемый процесс на данном уровне осуществляют с использованием определенного процесса (в том числе за счет сосредоточения внимания на сквозных областях функционального управления), который способен достичь выходов этого процесса. Предполагает оптимизацию процесса, связанного с управлением ИТ-активами, посредством информационных систем
Уровень 4 «Предсказуемый»	Описанный выше установленный процесс на данном уровне осуществляют, отслеживают и измеряют согласно сформулированным метрикам и кросс-функциональным ключевым показателям эффективности для достижения выходов этого процесса
Уровень 5 «Оптимизирующий»	Описанный выше установленный процесс на данном уровне означает, что организация осуществляет исследование новых методик и практик, обменивается опытом и усовершенствованными практиками для достижения выходов этого процесса.

Приложение В
(обязательное)

Процессы управления ИТ-активами

Процессы управления ИТ-активами следует рассматривать как неотъемлемую часть системы менеджмента сервисов согласно ГОСТ Р ИСО/МЭК 20000-1.

В данном приложении приведены:

- этапы управления жизненным циклом ИТ-активов;
- перечень взаимосвязанных процессов, задействованных в функционировании системы управления ИТ-активами.

На рисунке В.1 приведены этапы управления жизненным циклом ИТ-активов.

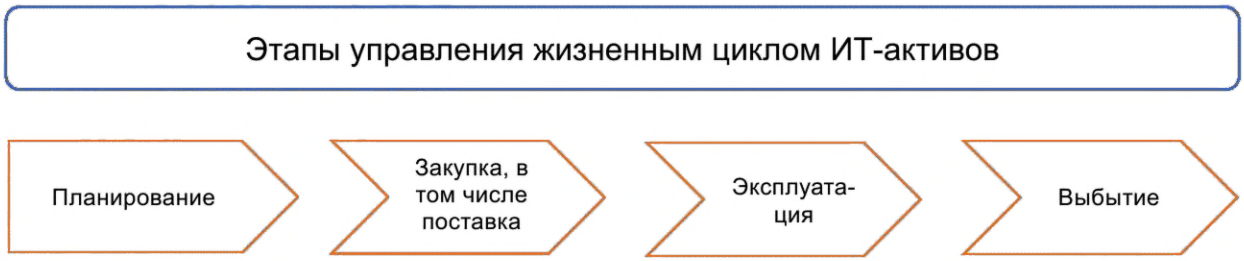


Рисунок В.1 — Этапы управления жизненным циклом ИТ-активов

На рисунке В.2 приведены взаимосвязанные процессы, задействованные в функционировании системы управления ИТ-активами.



Рисунок В.2 — Взаимосвязанные процессы,
задействованные в функционировании системы управления ИТ-активами

В таблице В.1 приведены цели этапов, структурированные по этапам жизненного цикла ИТ-активов; в таблице В.2 — области взаимодействия смежных процессов и управления ИТ-активами.

Таблица В.1 — Цели этапов жизненного цикла ИТ-активов

Этап	Цель этапов
Планирование	Цель данного этапа применительно к ИТ-активам — гарантировать, что потребность в ИТ-активах должным образом запрошена, проанализирована, оценена с точки зрения политики и технологической устойчивости и направлена на закупку
Закупка, в т. ч. поставка	Цель данного этапа применительно к ИТ-активам — гарантировать, что все ИТ-активы, запланированные к закупке, могут быть закуплены и своевременно размещены в местах хранения с ограниченным и контролируемым доступом персонала (склад, кабинет, помещение, сейф и т. п.) до момента ввода в эксплуатацию, а также на время распределения ИТ-активов в соответствии с потребностью и критичностью
Эксплуатация	Цель данного этапа применительно к ИТ-активам — гарантировать организацию учета и отслеживание ИТ-активов в течение всего срока эксплуатации, контроль и мониторинг актуальных статусов и данных по ключевым атрибутам об ИТ-активах, в т. ч. проведение периодической инвентаризации. В соответствие с данными, которые появляются в рамках этапа эксплуатации, осуществляется планирование дальнейших периодов модернизации, выбытия и т. п.
Выбытие	Цель данного этапа применительно к ИТ-активам — вывести ИТ-активы из эксплуатации (текущего использования) с последующим переназначением: - на списание; - на разукомплектацию; - на утилизацию/ликвидацию; - на передачу на благотворительность; - на перепродажу; - и другие (где это уместно в соответствии с политикой компании и соблюдением всех требований к ведению учета)

Таблица В.2 — Области взаимодействия смежных процессов и управления ИТ-активами

Процесс	Цели процесса
Управление изменениями	Данный процесс является источником данных по планируемым изменениям, вносимым в процессе перехода ИТ-активов из текущего состояния. Кроме того, осуществляется контроль за планируемыми изменениями, оцениваются последствия изменений относительно ИТ-активов с принятием при необходимости мер по смягчению неблагоприятных последствий
Управление данными	Данный процесс определяет порядок создания, хранения, поддержки данных, а также обеспечение доступа к данным. Кроме того, осуществляются хранение и отображение актуальных данных ИТ-активов для обеспечения возможности их анализа, интерпретации и обработки
Управление безопасностью	Данный процесс определяет требования к безопасности, относящиеся к управлению ИТ-активами, а также при его проведении осуществляется контроль соблюдения требований безопасности. Кроме того, соблюдаются правила, установленные управлением безопасности, и осуществляется контроль за соблюдением требований относительно ИТ-активов
Управление отношениями и контрактами	Данный процесс гарантирует бесперебойное предоставление качественных услуг по управлению ИТ-активами, а также управление всеми контрактами на ИТ-активы и услуги с соблюдением всех юридических норм и авторских прав для ИТ-активов в рамках процесса. Кроме того, информирует о выполнении условий контракта относительно ИТ-активов

Окончание таблицы В.2

Процесс	Цели процесса
Управление финансами	Данный процесс гарантирует, что финансовые затраты, связанные с ИТ-активами, отслеживаются и регулируются, в том числе на предмет экономической эффективности. Кроме того, предоставляются данные по плану управления ИТ-активами для качественного управления финансами
Управление уровнем услуг	Данный процесс определяет целевые показатели уровня сервисов, которым организация обязуется соответствовать. Кроме того, процесс содействует в соблюдении параметров ИТ-услуг при управлении ИТ-активами
Управление рисками	Данный процесс выявляет возможные риски, относящиеся к управлению ИТ-активами, формирует требования по их устранению. Кроме того, соблюдаются требования, установленные управлением рисками, и осуществляется контроль за соблюдением требований относительно ИТ-активов
Управление конфигурациями	Данный процесс является источником данных для поддержания в актуальном состоянии данных о конфигурационных единицах и взаимосвязях между ними. Кроме того, оценивается влияние изменения конфигурационных единиц на ИТ-инфраструктуру в целом и поддерживаются в актуальном состоянии данные о конфигурационных единицах относительно ИТ-активов
Управление мощностями ИТ-услуг	Данный процесс обеспечивает своевременное и эффективное планирование выделения ресурсов, оборудования и ПО для удовлетворения требованиям к ИТ-услугам. Кроме того, предоставляются актуальные данные об ИТ-активах для планирования

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 *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 27.06.2025. Подписано в печать 07.07.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru