ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 38500— 2017

Информационные технологии

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ В ОРГАНИЗАЦИИ

(ISO/IEC 38500:2015, IDT)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 8 сентября 2017 г. № 1041-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 38500:2015 «Информационные технологии. Стратегическое управление ИТ в организации» (ISO/IEC 38500:2015 «Information technology — Governance of IT for the organization», IDT).

ИСО/МЭК 38500 разработан подкомитетом ПК 40 «Управление информационными технологиями и услугами ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК)

5 ВВЕДЕН ВПЕРВЫЕ

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

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

Содержание

Введение

Международный стандарт ИСО/МЭК 38500:2015 разработан взамен ИСО/МЭК 38500:2008.

Целью настоящего стандарта является предоставление руководящим органам принципов, определений и модели для оценки, руководства, анализа и отслеживания использования информационных технологий (ИТ) в своих организациях.

Настоящий стандарт представляет собой высокоуровневый рекомендательный документ, определяющий принципы стратегического управления ИТ. Кроме того он обеспечивает общие инструкции в отношении роли руководящих органов, а также помогает организациям использовать соответствующие стандарты для осуществления стратегического управления ИТ.

Многие организации используют ИТ как важнейший инструмент бизнеса; в редких случаях организации могут эффективно работать без них. ИТ — также значительный фактор в будущих бизнес-планах многих организаций.

Затраты на ИТ могут составлять существенную долю финансовых и кадровых затрат организации. При этом возврат инвестиций от таких вложений часто не реализуется полностью, и отрицательное влияние на организацию может быть значительным.

Основные причины таких негативных результатов связаны с тем, что упор делается на технические, финансовые и плановые аспекты ИТ, а не на бизнес-контекст использования ИТ.

Настоящий стандарт описывает принципы, определения и модель для эффективного стратегического управления ИТ; он предназначен для помощи высшему руководству организаций в понимании и выполнении их юридических, регулирующих и этических обязательств в отношении использования ИТ в организациях.

Настоящий стандарт соответствует определению корпоративного стратегического управления, опубликованному в отчете Комитета по финансовым аспектам корпоративного управления («Отчет Кэдбери») в 1992 году. Этот отчет также обеспечил основу определения корпоративного стратегического управления в документе Организации экономического сотрудничества и развития (ОЭСР) «Принципы корпоративного управления», принятом в 1999 году (и пересмотренном в 2004 году). Корпоративное стратегическое управление и оперативное управление — разные понятия; во избежание путаницы в настоящем стандарте даются определения обоих понятий. Подробнее они рассматриваются в ИСО/МЭК ТО 38502.

Настоящий стандарт предназначен главным образом для руководящих органов. В некоторых организациях (обычно небольшого размера) члены руководящего стратегического органа одновременно могут быть операционными линейными руководителями. Настоящий стандарт применим во всех организациях, от самых маленьких до самых крупных, вне зависимости от их назначения, устройства и формы собственности.

Процесс внедрения стратегического управления ИТ приведен в ИСО/МЭК TS 38501.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ В ОРГАНИЗАЦИИ

Information technology.
Governance of IT for the organization

Дата введения — 2018—09—01

1 Область применения

Настоящий стандарт описывает руководящие принципы для членов руководящих органов организаций (которые могут включать собственников, директоров, партнеров, руководителей и пр.) по эффективному, действенному и приемлемому использованию информационных технологий (ИТ) в организации.

Настоящий стандарт также предоставляет рекомендации для лиц, ответственных за консультирование, информирование или помощь руководящим органам. В их число входят:

- руководители верхнего звена;
- члены групп, отслеживающих ресурсы в организации;
- внешние бизнес-специалисты или технические специалисты, например юристы и бухгалтеры, розничные или промышленные ассоциации, профессиональные сообщества;
- внутренние и внешние поставщики услуг (включая консультантов);
- аудиторы.

Настоящий стандарт применим к стратегическому управлению настоящим и будущим использованием ИТ, включая процессы управления и решения, относящиеся к настоящему и будущему. Эти процессы могут контролироваться собственными ИТ-специалистами организации, внешними поставщиками услуг или бизнес-подразделениями организации.

Настоящий стандарт определяет стратегическое управление ИТ как подмножество или область организационного стратегического управления, или в случае корпорации — корпоративного стратегического управления.

Настоящий стандарт применим к любым организациям, включая общественные и частные компании, государственные структуры и некоммерческие организации. Этот стандарт применим в организациях любого размера, от небольших до самых крупных, вне зависимости от степени использования ИТ.

Цель настоящего стандарта — способствовать эффективному, действенному и приемлемому использованию информационных технологий в организациях за счет следующих факторов:

- обеспечения уверенности заинтересованных лиц в том, что при соблюдении принципов и методик, предлагаемых настоящим стандартом, они могут доверять стратегическому управлению ИТ в своих организациях;
- информирования и ориентирования руководящих органов в отношении использования ИТ в их организациях;
- формирования словаря для стратегического управления ИТ.

Издание официальное

2 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1 **приемлемый** (acceptable): Отвечающий ожиданиям заинтересованных лиц, если можно продемонстрировать обоснованность и разумность этих ожиданий.

2.2 **ответственный** (accountable): Несущий ответственность за действия, решения и работоспособность.

2.3 **подотчетность** (accountability): Состояние ответственности.

Примечание — Состояние ответственности по отношению к установленной обязанности. Обязанность может основываться на нормативах, соглашении или назначении как части делегирования.

2.4 **корпоративное стратегическое управление** (corporate governance): Система, в которой корпорации управляются и контролируются.

Примечания

1 Это организационное управление, применяемое к корпорациям.

2 Из Отчета Кэдбери 1992 г. и документа ОЭСР 1999 г.

3 Определение включает разъяснение изменения терминологии по сравнению с предыдущей редакцией.

2.5 **направление** (direct): Взаимодействие с кем-либо для передачи желаемых целей и результатов.

Примечания

1 В контексте стратегического управления ИТ это подразумевает постановку целей, выработку стратегий и политик для принятия членами организации, чтобы обеспечить соответствие ИТ целям бизнеса.

2 Цели, стратегии и политики могут устанавливаться менеджерами, если руководящий орган делегировал им соответствующие полномочия.

2.6 **оценка** (evaluate): Рассмотрение и вынесение обоснованных заключений.

Примечание — В контексте стратегического управления ИТ оценка включает в себя заключения о внутренних и внешних, существующих и будущих обстоятельствах и возможностях, связанных с текущим и будущим использованием ИТ в организации.

2.7 **руководитель верхнего звена** (executive manager): Человек, которому руководящий орган делегирует полномочия по реализации стратегий и политик для достижения целей организации.

Примечания

1 К руководителям верхнего звена могут относиться сотрудники, подотчетные руководящему органу или главе организации либо несущие общую ответственность по основным направлениям деятельности. Например, исполнительный директор, руководитель государственной организации, финансовый директор, операционный директор, ИТ-директор и аналогичные руководители.

2 В стандартах менеджмента руководители верхнего звена могут называться топ-менеджерами.

2.8 **стратегическое управление** (governance): Система управления и контроля.

2.9 **руководящий орган** (governing body): Человек или группа людей, которые отвечают за работу организации и ее соответствие требованиям.

2.10 **стратегическое управление ИТ** (governance of IT): Система, при помощи которой осуществляется управление и контроль настоящим и будущим использованием ИТ.

Примечания

1 Стратегическое управление ИТ является одним из компонентов или подмножеством организационного стратегического управления.

2 Термин «стратегическое управление ИТ» эквивалентен терминам «корпоративное стратегическое управление ИТ», «стратегическое управление ИТ предприятия», а также «организационное стратегическое управление ИТ».

2.11 **поведение человека** (human behavior): Взаимодействие людей и других элементов системы.

Примечания

1 Поведение человека включает культуру, потребности и стремления как отдельных людей, так и групп.

2 В отношении ИТ существует множество сообществ или групп людей, каждое из которых имеет собственные потребности, стремления и поведение. Например, для людей, использующих информационные системы, характерны потребности, связанные с удобством пользования и эргономикой, а также с доступностью и производительностью. Люди, чьи должностные обязанности изменяются из-за использования ИТ, могут обладать потребностями, связанными с коммуникацией, обучением и ободрением. У людей, участвующих в создании и эксплуатации ИТ-ресурсов, могут быть потребности, связанные с условиями работы и развитием компетенций.

2.12 **информационные технологии (ИТ)** [information technology (IT)]: Ресурсы, используемые для получения, обработки, хранения и распространения информации.

Примечание — Это понятие также включает понятие «коммуникационные технологии» и составной термин «информационно-коммуникационные технологии» (ИКТ).

2.13 **инвестирование** (investment): Выделение ресурсов с целью достижения определенных целей и получения других выгод.

2.14 **менеджмент** или **оперативное управление** (management): Осуществление контроля и надзора в рамках полномочий и ответственности, установленных стратегическим управлением.

Примечание — Термин «менеджмент» часто используется в качестве собирательного определения для всех лиц, отвечающих за управление организацией или ее частями. Термин «менеджеры» используется во избежание путаницы с системами управления.

2.15 **руководители** (managers): Группа людей, отвечающих за контроль и надзор за организацией или ее частями.

Примечание — Руководители верхнего звена являются одной из категорий руководителей организации.

2.16 **отслеживание** (monitor): Отслеживание как основа принятия соответствующих решений и корректировок.

Примечания

1 Отслеживание включает в себя регулярное получение информации о выполнении планов, а также периодическую проверку итоговых достижений в реализации согласованных стратегий и получении результатов с целью обеспечения основы для принятия решений и корректировки планов.

2 Отслеживание включает в себя проверку соответствия релевантным требованиям законодательства, нормативам и политикам организации.

2.17

организация (organization): Человек или группа людей, наделенных собственными функциями, областями ответственности, полномочиями и взаимоотношениями для достижения своих целей.

Примечание — Понятие «организация» включает в себя, но не ограничивается такими формами, как индивидуальный предприниматель, компания, корпорация, фирма, партнерство, благотворительная организация или учреждение, или часть, или комбинация форм из этого списка вне зависимости от того, зарегистрирована ли организация в качестве юридического лица, является ли она государственной или частной.

[ИСТОЧНИК: Сводное дополнение ИСО. Специальные процедуры ИСО. Приложение SL, дополнение 2 [3]. Примечание добавлено в настоящий стандарт.]

2.18 **организационное управление** (organizational governance): Система, в соответствии к которой организации управляются и контролируются.

2.19 **политика** (policy): Намерения и направление развития организации, формально выраженное руководящим органом или руководителями верхнего звена, наделенными надлежащими полномочиями.

2.20 **предложение** (proposal): Комбинация выгод, затрат, рисков, возможностей и других факторов, применимых к принимаемым решениям.

Пример — бизнес-кейс.

2.21 **ресурсы** (resources): Люди, процедуры, программное обеспечение, информация, оборудование, расходные материалы, инфраструктура, капитальные и операционные фонды и время.

2.22 **ответственность** (responsibility): Обязанность действовать и принимать решения для достижения требуемых результатов.

2.23

риск (release): Влияние неопределенности на достижение целей.

Примечания

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

2 Отрицательное влияние означает угрозы, в то время как положительное — возможности.

[Руководство ИСО 73:2009]

2.24

заинтересованное лицо (stakeholder): Любой человек, группа или организация, которые могут влиять или подвергаться влиянию, или ощущать себя подвергнувшимися влиянию какого-либо решения или действия.

[Адаптировано из Руководства ISO 73:2009]

2.25 **использование ИТ** (use of IT): Планирование, проектирование, разработка, развертывание, эксплуатация, управление и применение ИТ для выполнения задач бизнеса и создания ценности для организации.

Примечания

1 Использование ИТ подразумевает как спрос в области ИТ, так и предложение в этой области.

2 Использование ИТ относится как к текущему, так и будущему использованию.

3 Преимущества эффективного стратегического управления ИТ

Эффективное стратегическое управление ИТ помогает руководящим органам удостовериться в том, что использование ИТ положительно влияет на работоспособность организации за счет следующих факторов:

- инноваций в услугах, на рынках, в бизнесе;
- выравнивания ИТ с потребностями бизнеса;
- надлежащего внедрения и эксплуатации ИТ-активов;
- прозрачности в ответственности и подотчетности как в отношении предложения ИТ, так и спроса на ИТ, для достижения целей организации;
- непрерывности бизнеса и его стабильности;
- эффективного выделения ресурсов;
- эффективных взаимоотношений с заинтересованными лицами;
- достижения на практике ожидаемых выгод от каждой инвестиции в ИТ.

Настоящий стандарт устанавливает принципы эффективного, действенного и приемлемого использования ИТ. Руководящие органы, добившись выполнения этих принципов в организациях, получат помощь в управлении рисками и реализации возможностей, возникающих благодаря использованию ИТ.

Эффективное стратегическое управление ИТ также помогает руководящим органам обеспечивать соответствие обязательным требованиям (регулирующих органов, законодательства, договорных обязательств) в отношении приемлемого использования ИТ.

Настоящий стандарт определяет модель стратегического управления ИТ. Риск невыполнения руководящими органами своих обязательств смягчается за счет внимания к модели в части надлежащего применения принципов.

Неправильное внедрение ИТ-систем, неверное или несоответствующее использование ИТ может подвергнуть организацию риску несоответствия законодательству. Например, в некоторых юрисдикциях члены руководящих органов могут нести личную ответственность за неадекватные результаты работы бухгалтерской системы, приведшие к неуплате налога.

Процессы работы с ИТ включают определенные риски, которые должны быть рассмотрены соответствующим образом. Например, руководящие органы и их члены могут нести ответственность в следующих случаях:

- нарушение законодательства и нормативных требований, касающихся конфиденциальности, нежелательной почты (спама), здоровья и безопасности, документации;
- несоответствие стандартам, относящимся к безопасности, социальной ответственности;
- возникновение вопросов, связанных с правами интеллектуальной собственности, включая лицензионные соглашения.

Руководящие органы, использующие рекомендации этого стандарта, с большей вероятностью выполнят свои обязательства.

4 Принципы и модель эффективного стратегического управления ИТ

4.1 Принципы

В подразделе представлено шесть принципов эффективного стратегического управления ИТ. Эти принципы определяют предпочтительное поведение, которым следует руководствоваться при принятии

решений. Каждый принцип описывает, что должно происходить, но не описывает, каким образом, когда и кем должны быть реализованы эти принципы, поскольку такие аспекты в значительной мере зависят от природы организации, реализующей эти принципы. Руководящие органы должны требовать применения этих принципов.

Принцип 1. Ответственность

Лица и группы лиц в организации должны понимать и брать на себя ответственность в отношении как предложения ИТ, так и спроса на ИТ. Лица, ответственные за те или иные действия, должны обладать полномочиями на выполнение этих действий.

Принцип 2. Стратегия

Стратегия бизнеса организации должна учитывать существующие и будущие возможности ИТ; планы использования ИТ должны соответствовать текущим и планируемым потребностям стратегии бизнеса организации.

Принцип 3. Приобретение

Приобретение ИТ-активов должно проводиться по убедительным причинам, на основе надлежащего и непрерывного анализа, с четким и прозрачным принятием решений. Существует необходимый баланс между выгодами, возможностями, затратами и рисками, как в краткосрочной, так и долгосрочной перспективе.

Принцип 4. Эффективность

ИТ должны быть пригодны для поддержки организации, предоставления услуг, уровней сервиса и качества обслуживания, необходимых для удовлетворения текущих и будущих требований бизнеса.

Принцип 5. Соответствие требованиям

Использование ИТ должно соответствовать всем обязательным законодательным и нормативным требованиям. Методики и политики должны быть четко определены, внедрены и реализованы.

Принцип 6. Поведение человека

Политики, практики и решения ИТ должны демонстрировать уважение к поведению людей, включая существующие и будущие потребности всех задействованных в процессе лиц.

4.2 Модель

Руководящие органы должны управлять ИТ посредством трех основных задач:

а) оценки текущего и будущего использования ИТ;

в) направления подготовки и внедрения стратегий и политик, чтобы гарантировать соответствие ИТ целям бизнеса;

с) отслеживания соответствия политикам и эффективности стратегии.

Полномочия в отношении отдельных аспектов ИТ могут быть делегированы операционным руководителям организации. Тем не менее руководящий орган всегда несет ответственность за эффективное, действенное и приемлемое использование ИТ в организации, и эта ответственность не может быть делегирована.

Модель управления ИТ с помощью триады Оценка — Направление — Отслеживание приведена на рисунке 1. Пояснения изображенных на рисунке элементов и связей между ними приведены в тексте после рисунка.

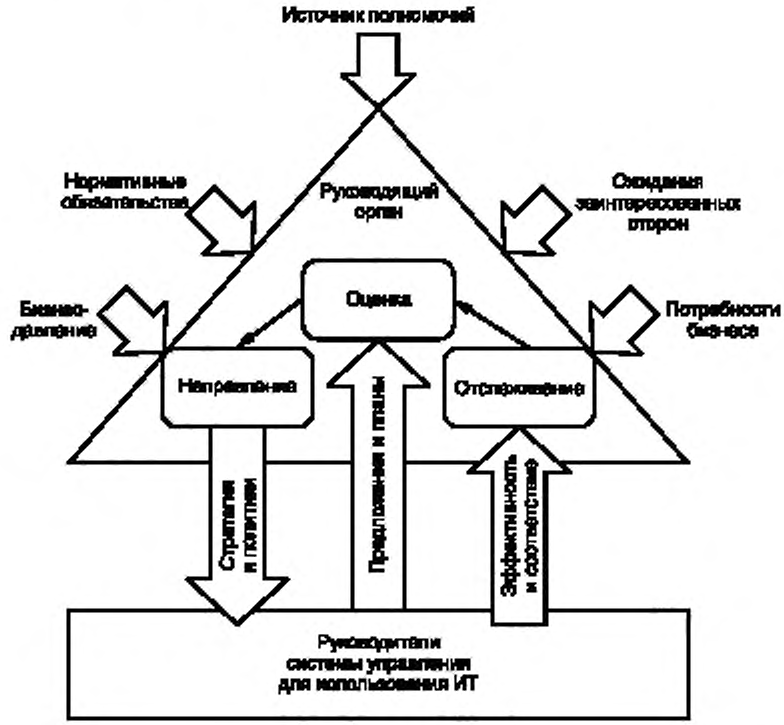

Рисунок 1 — Модель управления ИТ

Оценка

Руководящие органы должны изучать и оценивать существующее и будущее использование ИТ, включая планы, предложения и механизмы снабжения (внутренние, внешние или и те, и другие).

При оценке использования ИТ руководящие органы должны учитывать внешнее и внутреннее давление на организацию, такое как технологические изменения, экономические и социальные тенденции, нормативные обязательства, закономерные ожидания заинтересованных сторон, политическое влияние. Руководящие органы должны непрерывно проводить оценку по мере изменения обстоятельств. Руководящие органы также должны учитывать существующие и будущие потребности бизнеса: существующие и будущие цели организации, которых она должна достигнуть, такие как поддержание конкурентного преимущества, а также выполнение специфических целей, оценку планов и предложений.

Направление

Руководящие органы должны назначать ответственных и напрямую подготавливать и реализовывать стратегии и политики. Стратегии должны устанавливать направление инвестиций в ИТ и цели ИТ. Политики должны устанавливать правильное поведение при использовании ИТ.

Руководящие органы должны поощрять культуру эффективного стратегического управления ИТ в своих организациях, требуя от линейных руководителей предоставлять своевременную информацию, следовать стратегическим направлениям и соблюдать шесть принципов эффективного стратегического управления.

При необходимости руководящие органы должны напрямую подавать предложения по удовлетворению выявленных потребностей.

Отслеживание

Руководящие органы должны отслеживать эффективность ИТ с помощью соответствующих измерительных систем. Руководящие органы должны убедиться в том, что функционирование соответствует стратегиям, в частности, в отношении целей бизнеса.

Руководящие органы также должны удостовериться, что ИТ соответствует внешним требованиям (регулирующих органов, законодательства, договорных обязательств) и внутренним практикам работы.

5 Руководство по стратегическому управлению ИТ

5.1 Общие положения

В следующих разделах приводится руководство для общих принципов управления ИТ и методики, необходимые для внедрения этих принципов.

Описанные методики не являются исчерпывающими, но предоставляют отправную точку для обсуждения ответственности руководящего органа за стратегическое управление ИТ. Таким образом, описанные методики предоставляют руководство для стратегического управления ИТ.

Каждая организация в отдельности индивидуально несет ответственность за определение конкретных действий, необходимых для реализации принципов, с учетом природы организации и соответствующего анализа рисков и возможностей использования ИТ.

5.2 Принцип 1. Ответственность

Оценка

Руководящие органы должны оценивать варианты назначения ответственных с учетом текущего и будущего использования ИТ в организации. При этом следует стремиться к эффективному, действенному и приемлемому использованию ИТ и к поддержке существующих и будущих целей бизнеса.

Руководящие органы должны оценивать компетентность ответственных лиц, которые принимают решения в отношении ИТ. Как правило, эти лица должны быть линейными бизнес-руководителями, также отвечающими за работу организации и достижение бизнес-целей; им должны помогать ИТ-специалисты, понимающие ценность ИТ для бизнеса и процессы организации.

Направление

Руководящие органы должны направлять деятельность таким образом, чтобы назначенные ответственными за ИТ лица следовали надлежащим стратегиям.

Руководящие органы должны обеспечить получение этими ответственными лицами информации, необходимой им для выполнения своих обязанностей и предоставления отчетности.

Отслеживание

Руководящие органы должны отслеживать внедрение соответствующих механизмов стратегического управления ИТ.

Руководящие органы должны следить за тем, чтобы ответственные лица признавали и понимали свои обязанности.

Руководящие органы должны отслеживать деятельность таких лиц в области стратегического управления ИТ (например, это касается людей, участвующих в работе комитетов управления или представляющих предложения руководящим органам).

5.3 Принцип 2. Стратегия

Оценка

Руководящие органы должны оценивать развитие ИТ и бизнес-процессов, чтобы убедиться в способности ИТ обеспечивать поддержку будущих нужд бизнеса.

Рассматривая планы и политики, руководящий орган должен оценивать использование ИТ и деятельность ИТ, чтобы убедиться в их соответствии целям организации и в удовлетворении ключевых правомерных требований заинтересованных лиц. Руководящий орган также должен принимать во внимание лучшие практики.

Руководящие органы должны убедиться, что использование ИТ учтено соответствующим образом в управлении рисками организации.

Направление

Руководящие органы должны управлять подготовкой и использованием стратегий и политик, обеспечивающих получение организацией выгод от развития ИТ.

Руководящие органы также должны поощрять предоставление предложений для инновационного использования ИТ, благодаря которым организация сможет реагировать на новые возможности, осваивать новые направления бизнеса или совершенствовать свои процессы.

Отслеживание

Руководящие органы должны отслеживать внедрение утвержденных предложений в области ИТ, следя за достижением поставленных целей в необходимые сроки с использованием выделенных ресурсов.

Руководящие органы должны отслеживать использование ИТ, чтобы убедиться в достижении предполагаемых выгод.

5.4 Принцип 3. Приобретение

Оценка

Руководящие органы должны оценивать различные варианты обеспечения ИТ, чтобы реализовывать утвержденные предложения, сбалансировать риски и обеспечить окупаемость предложенных инвестиций.

Направление

Руководящие органы должны направлять приобретение ИТ-активов (систем и инфраструктуры) соответствующим образом, включая подготовку необходимой документации, чтобы убедиться в обеспечении требуемых характеристик.

Руководящие органы должны следить за тем, чтобы договоренности о поставках (включая и внутренние, и внешние) поддерживали нужды бизнеса организации.

Руководящие органы должны позаботиться о том, чтобы организация и поставщики выработали совместное понимание намерений организации при осуществлении закупок, связанных с ИТ.

Отслеживание

Руководящие органы должны контролировать инвестиции в ИТ, следя за тем, чтобы все приобретаемые ИТ-активы имели требуемые характеристики.

Руководящие органы должны следить за тем, насколько успешно организация и поставщики поддерживают совместное понимание намерений организации при осуществлении любых закупок, связанных с ИТ.

5.5 Принцип 4. Эффективность

Оценка

Руководящие органы должны оценивать планы, предложенные линейными руководителями, чтобы убедиться в том, что ИТ будут поддерживать бизнес-процессы в соответствии с требуемыми функциями и работоспособностью. Эти предложения должны удовлетворять нуждам непрерывной нормальной работы организации и учитывать риски, связанные с использованием ИТ.

Руководящие органы должны оценивать риски непрерывности бизнеса, связанные с ИТ.

Руководящие органы должны оценивать риски целостности информации и защищенности ИТ-активов, включая риски, связанные с правами интеллектуальной собственности и организационными архивами.

Руководящие органы должны оценивать различные возможности принятия эффективных и своевременных решений, относящихся к использованию ИТ для поддержки целей бизнеса.

Руководящие органы должны регулярно оценивать эффективность и действенность стратегического управления ИТ в организации.

Направление

Руководящие органы должны обеспечивать выделение достаточных ресурсов, так чтобы ИТ удовлетворяли потребности организации в соответствии с выбранными приоритетами и бюджетными ограничениями.

Руководящие органы должны управлять ответственными лицами, чтобы обеспечить поддержку ИТ организации, когда это требуется по соображениям бизнеса, путем предоставления верных и актуальных данных, защищенных от потерь или неправильного использования.

Отслеживание

Руководящие органы должны отслеживать, в какой степени ИТ поддерживают бизнес. Руководящие органы должны следить, насколько приоритет выделения ресурсов и бюджета соответствует целям бизнеса.

Руководящие органы должны отслеживать, в какой степени соблюдаются политики, касающиеся, например, точности данных и эффективного использования ИТ.

5.6 Принцип 5. Соответствие требованиям

Оценка

Руководящие органы должны регулярно оценивать, насколько ИТ соответствуют требованиям (регулирующих органов, законодательства, договорных обязательств), внутренним политикам, стандартам и профессиональным руководствам.

Руководящие органы должны регулярно оценивать внутреннее соответствие организации принятой структуре стратегического управления ИТ.

Направление

Руководящие органы должны управлять ответственными лицами в формировании стандартных и типовых механизмов для уверенности в том, что ИТ соответствует релевантным требованиям, внутренним политикам, стандартам и правилам.

Руководящие органы должны добиться внедрения и применения политик, дающих организации возможность выполнять свои внутренние обязательства в отношении использования ИТ.

Руководящие органы должны добиться соблюдения ИТ-персоналом применимых правил профессионального поведения и развития.

Руководящие органы должны обеспечить соблюдение норм этики, относящихся к ИТ.

Отслеживание

Руководящие органы должны отслеживать соответствие ИТ требованиям посредством надлежащей отчетности и аудита; проверки должны быть своевременными, всесторонними и пригодными для оценки удовлетворенности организации.

Руководящие органы должны отслеживать деятельность в области ИТ, включая ликвидацию активов и данных, чтобы гарантировать соблюдение всех требований, касающихся экологии, конфиденциальности, стратегического управления знаниями, организационных архивов, а также прочих применимых требований.

5.7 Принцип 6. Поведение человека

Оценка

Руководящие органы должны оценивать деятельность в области ИТ, с тем чтобы идентифицировать и надлежащим образом рассматривать поведение людей.

Направление

Руководящие органы должны следить за тем, чтобы деятельность в области ИТ соответствовала установленным моделям поведения.

Руководящие органы должны добиться того, чтобы все сотрудники могли в любое время выявлять риски, возможности, проблемы и затруднения и сообщать о них. Управление этими рисками должно осуществляться согласно опубликованным политикам и процедурам и передаваться соответствующим лицам, принимающим решения.

Отслеживание

Руководящие органы должны контролировать деятельность в области ИТ, следя за тем, чтобы принятые модели поведения оставались действенными, и что им уделяется должное внимание.

Руководящие органы должны отслеживать практики работы, чтобы убедиться в их соответствии правилам надлежащего использования ИТ.

Библиография

[1] ISO/IEC TR 38502, Information technology — Governance of IT — Framework and model

[2] ISO/IEC TS 38501, Information technology — Corporate governance of IT — Implementation guide

[3] ISO/IEC Directives Part 1, Consolidated ISO Supplement, 2013, Annex SL, Appendix 2

[4] Report of the Committee on the Financial Aspects of Corporate Governance. Sir Adrian Cadbury, London, 1992

[5] OECD. Principles of Corporate Governance. OECD, 1999 and 2004

УДК 004:006.034 ОКС 35.020 IDT

Ключевые слова: информационные технологии (ИТ), модель управления ИТ, принципы управления ИТ, руководство по управлению ИТ

БЗ 7—2017/13

Редактор *К.В. Колесникова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 11.09.2017. Подписано в печать 02.10.2017. Формат 60×84 1/8. Гарнитура Ариал
Усл. печ. л. 1,86. Уч.-изд. л. 1,68. Тираж 25 экз. Зак. 1686.
Подготовлено на основе электронной версии предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4
www.gostinfo.ru info@gostinfo.ru