ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 58608— 2019/ ISO/IEC TR 38502:2017

Информационные технологии

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ

Структура и модель

(ISO/IEC TR 38502:2017, IDT)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС») и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 октября 2019 г. № 1030-ст

4 Настоящий стандарт идентичен международному документу ISO/IEC TR 38502:2017 «Информационные технологии. Стратегическое управление ИТ. Структура и модель» (ISO/IEC TR 38502:2017 «Information technology — Governance of IT — Framework and model», IDT).

ISO/IEC TR 38502 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 документа, 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

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Модель и структура 2
4.1 Модель стратегического управления ИТ 2
4.2 Взаимосвязь между стратегическим и оперативным управлением ИТ 3
4.3 Основные элементы системы стратегического управления ИТ 4
5 Руководство по использованию модели 5
5.1 Обязанности руководящего органа 5
5.2 Разработка стратегии и контроль 6
5.3 Делегирование 6
5.4 Обязанности руководителей 7
5.5 Стратегическое управление и внутренний контроль 8
Приложение А (справочное) Принципы надлежащего стратегического управления ИТ 9
Библиография 10

Введение

Успех любых инвестиций в информационные технологии (ИТ), будь то новые инициативы или существующие операции, определяется выгодой, которую они приносят организации-инвестору.

Как правило, выгоды от инвестиций в ИТ напрямую не вытекают из предоставляемых или поддерживаемых ИТ. Скорее всего, полученные выгоды являются результатом изменений деятельности организации, которые стали возможны при использовании технологии для удовлетворения требований или потребностей организации. Организации нуждаются в стратегии и механизмах поддержки ИТ, которые обеспечивают максимальную отдачу от инвестиций в ИТ при одновременном управлении рисками, связанными с использованием ИТ. Риски включают в себя неспособность достигнуть требуемой мощности, неспособность бизнеса извлечь необходимые выгоды, наличие сбоев в функционировании ИТ, которые могут дестабилизировать бизнес, привести к невыполнению обязательств, несоблюдению нормативных требований, сбоям безопасности, потере данных, простою и т. д.

Одна из задач, стоящих перед организацией в области инвестиций в ИТ, заключается в обеспечении того, чтобы эти инвестиции и решения о приобретении основывались на бизнес-стратегиях, приоритетах и потребностях организации. Поэтому те, кто отвечает за стратегическое управление организацией, должны осуществлять надлежащий контроль и вовлекаться в принятие решений, касающихся использования ИТ в бизнесе, с тем чтобы такие решения основывались на бизнес-стратегиях, приемлемом риске, приоритетах и потребностях организации. Усилия, которые требуются для получения ожидаемых выгод, должны быть определены и понятны.

ИСО/МЭК 38500 [1] признает, что обеспечение надлежащего баланса спроса и предложения ИТ требует от топ-менеджмента организации грамотного стратегического и оперативного управления. Целью ИСО/МЭК 38500 является предоставление руководящему органу методов по оценки, управления и мониторинга использования ИТ в организации.

Понятие «стратегическое управление» применительно к ИТ часто используют неправильно. Например, довольно часто термин «стратегическое управление» заменяют на термины «системы менеджмента», «структуры управления» и «информационные системы», которые сами по себе не относятся к стратегическому управлению, но которые одновременно являются результатами проведения и необходимыми инструментами эффективного стратегического управления. В результате очень часто возникает путаница в понимании функций стратегического и оперативного управления, и это затрудняет разработку непротиворечивой системы стратегического управления и для внедрения эффективных методов стратегического управления в организации.

Настоящий стандарт разработан с целью разъяснения различий между концепциями стратегического управления и операционного управления в области ИТ. В стандарте представлена модель, иллюстрирующая отношения между стратегическим управлением и оперативным управлением и определяющая ответственность каждого типа управления.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИТ

Структура и модель

Information technology. Governance of IT. Framework and model

Дата введения — 2021—01—01

1 Область применения

Настоящий стандарт предоставляет руководство по природе и механизмам стратегического и оперативного управления, а также их взаимосвязи, в контексте информационных технологий (ИТ) в организации.

Цель настоящего стандарта заключается в предоставлении информации о структуре и моделях, которые могут использоваться для определения ограничений и взаимосвязей между стратегическим и операционным управлением как в текущем периоде, так и в будущем, при использовании ИТ.

Стандарт предоставляет руководство для следующего круга лиц:

- руководящих органов;
- руководителей, чьи компетенции и ответственность связаны со стратегическим управлением;
- советников или тех, кто осуществляет помощь в стратегическом управлении организаций всех размеров и типов;
- разработчиков стандартов в области стратегического и оперативного управления ИТ.

2 Нормативные ссылки

Настоящий стандарт не содержит нормативных ссылок.

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 38500, а также следующие термины с соответствующими определениями.

ИСО и МЭК ведут терминологические базы данных в области стандартизации по следующим адресам:

- IEC Electropedia: см. https://www.electropedia.org/
- ISO онлайн доступ: см. https://www.iso.org/obp

3.1 **структура стратегического управления** (governance framework): Стратегии, политики, системы принятия решений и подотчетность, с помощью которых осуществляется функционирование управленческих механизмов организации.

3.2 **внутренний контроль** (internal control): Политика, внутренние процедуры, практика и организационные структуры, разработанные для обеспечения гарантий достижения целей бизнеса и для выявления, предотвращения и исправления неблагоприятных событий.

Издание официальное

3.3

система менеджмента (management system): Совокупность взаимозависимых и взаимосвязанных элементов организации, направленных на формирование политик и целей, а также процессов достижения этих целей.

Примечания

1 Система менеджмента может рассматривать отдельную дисциплину или несколько дисциплин.

2 Системы менеджмента должны функционировать внутри стратегий, структур, обязанностей и подотчетности, описанных в структуре стратегического управления.

[ИСО 9000:2015, статья 3.5.3, изменения в примечаниях]

3.4

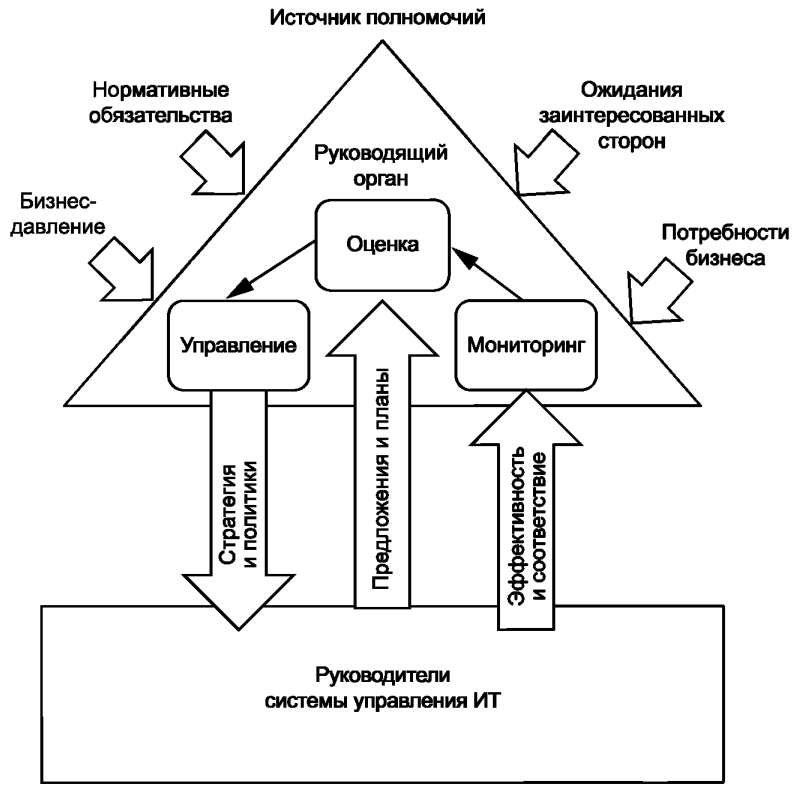
риск-аппетит (risk appetite): Величина и тип риска, приемлемого для организации.
[ISO Guide 73:2009, статья 3.7.1.2]

4 Модель и структура

4.1 Модель стратегического управления ИТ

4.1.1 Обязанности и подотчетность руководящего органа

Руководящий орган несет ответственность и контролирует результаты текущего и будущего использования ИТ в организации, что входит в его обязанности по стратегическому управлению организацией.



Примечание — Источник: ИСО/МЭК 38500.

Рисунок 1 — Модель стратегического управления ИТ

Полномочия, обязанности и подотчетность руководящего органа будут зависеть от источника полномочий, такого как законодательный механизм, в рамках которого он функционирует. Допустимый

уровень полномочий и ограничения деятельности организации обычно задокументированы. В зависимости от размера, типа организации и законодательной базы, применимой к ней, в качестве такой документации используют учредительный договор, устав или обычное соглашение между сторонами.

Во многих акционерных обществах руководящим органом является совет, например, совет директоров. Существуют определенные юрисдикции, в которых используется двухуровневая структура с наблюдательным и исполнительным советами.

4.1.2 Задачи стратегического управления

В ИСО/МЭК 38500 [1] представлены рекомендации руководящему органу по решению с помощью ИТ следующих задач:

- оценки;
- управления;
- мониторингу.

Осуществление задач по оценке, управлению и мониторингу результатов организации происходит в тесном сотрудничестве руководящего органа и руководителей, с тем чтобы руководящий орган осуществлял управление и контроль использования ИТ для достижения целей бизнеса.

Осуществляя стратегическое управление, руководящий орган должен учитывать нормативные требования и законные ожидания заинтересованных лиц, наряду с влиянием внешней деловой среды, включая бизнес-давление и бизнес-требования.

4.1.3 Обязанности и подотчетность руководителей

В обязанности руководителей входит достижение целей организации в рамках политик и стратегий, установленных руководящим органом. Руководители подотчетны руководящему органу в отношении возложенных на них обязанностей.

Организации могут функционировать в иерархической структуре управления, в которой генеральный директор, несет полную ответственность, а другие руководители организации отчитываются перед ним напрямую или через других руководителей в установленном порядке. В некоторых организациях назначенные исполнительные руководители являются частью руководящего органа.

4.1.4 Применимость модели

Модель стратегического управления ИТ, описанная в этом разделе, может также использоваться в качестве требований к стратегическому управлению в организациях, в которых отсутствует формальный руководящий орган, такой как совет директоров. К таким организациям могут относиться правительственные организации, в которых полномочия, обязанности и подотчетность относятся к политической системе государства. В таких ситуациях полномочия и обязанности по стратегическому управлению могут делегироваться напрямую одному или нескольким исполнительным руководителям организации. Обычно таким руководителем является генеральный директор (или руководитель схожего уровня), который принимает на себя функции руководящего органа. В малом бизнесе роль руководящего органа и генерального директора может выполнять одно и то же лицо.

4.2 Взаимосвязь между стратегическим и оперативным управлением ИТ

Ключевыми элементами взаимодействия между стратегическим и оперативным управлением ИТ в соответствии с моделью, являются:

a) обязанности руководящего органа. Члены руководящего органа отвечают за стратегическое управление ИТ и несут ответственность за эффективное, результативное и допустимое использование ИТ в организации;

b) формулировка стратегии и контроль ее исполнения. Стратегическое управление обеспечивает способы, с помощью которых руководящий орган устанавливает направление деятельности организации в отношении использования ИТ и отслеживает состояние организации и эффективность руководителей в отношении достижения требуемых результатов;

c) делегирование. Аспекты стратегического управления ИТ могут выполняться руководителями, если за ними закреплены соответствующие обязанности, переданными им руководящим органом вместе с делегированными полномочиями;

d) обязанности руководителей. В обязанности руководителей входит достижение стратегических целей организации в соответствии со стратегиями и политиками использования ИТ, утвержденными руководящим органом;

e) стратегическое управление и внутренний контроль. Для эффективного стратегического управления ИТ необходима эффективная система внутреннего контроля как часть систем управления организацией.

Каждый из этих элементов подробно описан в разделе 5 «Руководство по использованию модели».

4.3 Основные элементы системы стратегического управления ИТ

Системы управления ИТ в организации ИТ и их использование должны быть основаны на системе стратегического управления организацией.

Фактическая система стратегического управления будет определяться самой организацией и зависит от ее размера и функций, а также решений руководящего органа относительно зоны ответственности, но основные элементы должны соответствовать рисунку 2. Заштрихованная область соответствует элементам управления.

Рисунок 2 — Основные элементы системы стратегического управления ИТ

Основные элементы системы стратегического управления ИТ должны включать в себя:

a) принципы надлежащего стратегического управления ИТ. Система стратегического управления должна основываться на принципах для надлежащего стратегического управления ИТ, как описано в ИСО/МЭК 38500 (приложение А настоящего стандарта). Данные принципы должны помогать организации в определении стратегического управления в области использования ИТ;

b) стратегии и политики использования ИТ в организации. Стратегии и политики использования ИТ устанавливаются руководящим органом и передаются руководителям для обеспечения основы применения стратегического управления ИТ для систем управления организации. Несмотря на то, основаны ли они на обязательных требованиях законодательства и нормативных правилах в различных юрисдикциях или на требованиях для организаций частного сектора, стратегии и политики должны учитывать специфические требования руководящего органа и руководителей организации. Стратегии и политики, основанные на принципах поведения, описанных в ИСО/МЭК 38500, должны быть определены, распространены, и результаты их использования проверены. Они могут включать в себя:

- бизнес-цели для использования ИТ;

- приоритеты и выделенные ресурсы;
- уровень полномочий и права принятия решений, включая зарезервированные для руководящего органа права;
- необходимые действия для принятия решений на основе согласованных стратегий и политик использования ИТ, в том числе обязанности, ограничения, полномочия, исключительные ситуации и отчетность;
- уровень риск-аппетита относительно использования ИТ, и специфические требования контроля рисков;
- политики, которые определяют требуемое поведение в отношении использования ИТ;

c) бизнес-планирование для ИТ. Процессы бизнес-планирования должны учитывать текущие и будущие возможности ИТ для обеспечения соответствия стратегического плана ИТ текущим и действующим потребностям бизнес-стратегии организации. Бизнес-планирование включает в себя бизнес-инновации, которые доступны с помощью ИТ. Следовательно, бизнес-планирование для ИТ является неотъемлемой частью системы стратегического управления ИТ в организации;

d) управление рисками. Система стратегического управления ИТ должна включать в себя надежные практики управления рисками, охватывающие все действия, связанные с ИТ, и принятие решений в этой области. Управление рисками в области ИТ должно основываться на общих принципах управления рисками в организации;

e) отчетность. Необходимо определить и утвердить механизмы предоставления отчетности. Данный процесс может включать в себя текущую оценку эффективности (как эффективности, так и соответствия требованиям) ИТ стратегий, планов и бизнес-подразделений организации;

f) системы оперативного управления ИТ. Системы оперативного управления ИТ должны функционировать в рамках стратегий и политик, определенных руководящим органом для достижения стратегических и оперативных целей организации. Эти системы включают в себя спрос на ИТ и предложение ИТ для внутренних подразделений организации, специализированных подразделений ИТ организации или внешних поставщиков и внешние сервисные организации. Ответственность за внедрение систем оперативного управления для достижения целей организации лежит на руководителях организации;

g) использование ИТ в организации. Фокус системы стратегического управления ИТ сосредоточен на использовании ИТ. Использование ИТ, соответствующее потребностям бизнеса, должно быть предметом стратегий и политик, определенных как часть системы стратегического управления, так же как систем оперативного управления ИТ в организации.

Система стратегического управления должна предоставлять руководителям возможность действовать максимально свободно при выполнении ежедневных задач. Стратегическое управление подразумевает общие ценности и цели, определение направления, обеспечение ресурсами и делегирование полномочий для того, чтобы руководители могли действовать автономно и с надлежащей оперативностью в изменяющейся среде.

5 Руководство по использованию модели

5.1 Обязанности руководящего органа

5.1.1 Общие положения

Члены руководящего органа несут ответственность за стратегическое управление ИТ и отвечают за эффективность, результативность и допустимое использование ИТ в организации. [4.2 a)]

Полномочия, обязанности и ответственность руководящего органа за эффективное, результативное и допустимое использование ИТ вытекают из общих полномочий по стратегическому управлению организацией.

Ключевая роль руководящего органа в стратегическом управлении ИТ заключается в обеспечении получения ценности от инвестиций в ИТ с учетом управления рисками.

5.1.2 Руководящий орган и механизмы контроля

a) Руководящий орган должен разработать механизмы контроля стратегического управления ИТ, которые соответствуют уровню зависимости бизнеса от ИТ.

b) Руководящий орган должен иметь ясное понимание важности ИТ для стратегии бизнеса организации, также как потенциального стратегического риска организации при использовании ИТ. Степень внимания руководящего органа к ИТ должна основываться на этих факторах.

c) Руководящий орган может сформировать подкомитет для помощи по контролю за использованием ИТ в организации со стратегической точки зрения. Необходимость в создании подкомитета зависит от важности ИТ для организации, а также от размера организации.

d) Руководящий орган должен обеспечить необходимые знания и понимание использования ИТ, а также будущих трендов и направлений ИТ, своими членами и представителями управляющих подразделений. (таких как комитеты по аудиту, по управлению рисками и контролю ИТ) также как соответствие их компетенций возложенным на них обязанностям.

e) Руководящий орган должен контролировать результативность механизмов стратегического управления ИТ, с помощью необходимых процессов, таких как аудит и независимая оценка, чтобы подтвердить эффективность стратегического управления. Например, руководящий орган должен удостовериться, что адекватный аудит охватывает управление рисками, связанными с ИТ, процессы контроля и стратегического управления.

5.2 Разработка стратегии и контроль

5.2.1 Общие положения

Стратегическое управление обеспечивает способы, с помощью которых руководящий орган устанавливает направление деятельности организации в отношении использования ИТ и отслеживает состояние организации и эффективность руководителей в отношении достижения требуемых результатов. [4.2b)]

В целом, руководящий орган руководит организацией, разрабатывая стратегию и контролируя эффективность руководителей при ее осуществлении. Во многих организациях для этого требуется, чтобы руководящий орган работал совместно с исполнительными руководителями и советовался с ними. Совместно они могут выработать ясное понимание того, как наилучшим образом использовать ИТ для получения выгод, как в настоящем, так и в будущем.

5.2.2 Роль управляющего органа при разработке стратегии

a) Руководящий орган, работая совместно и советуясь с исполнительными руководителями, должен обеспечить лидерство в разработке стратегии для получения выгод от использования ИТ.

b) Руководящий орган должен утвердить бизнес-стратегию для ИТ в организации, учитывая значение стратегии для достижения бизнес-целей и связанные с этим риски, которые могут возникнуть.

c) Руководящий орган должен удостовериться, что внутренняя и внешняя среда организации регулярно отслеживается и анализируется для выявления потребности в пересмотре и, когда уместно, изменении стратегии ИТ и связанных с ней политик. Причиной пересмотра или изменения стратегии могут послужить потребности и ожидания клиентов, конкурентная ситуация, сильные и слабые стороны организации, а также ее возможности, новые технологии, требования законодательства, политические изменения, экономические прогнозы и социологические факторы.

d) Руководящий орган должен обеспечить разработку политик для руководства организацией. Такие политики должны поддерживать достижение бизнес-целей, включая в себя обязательные требования законодательства и нормативные требования. Политики могут основываться на лучших практиках и предписывать руководство организацией с точки зрения управления рисками или улучшать эффективность и результативность организации.

e) Руководящий орган должен обеспечить наличие механизмов, разъяснения и интерпретации целей, стратегий и политик по мере их возникновения.

f) Руководящий орган должен понимать готовность организации к любым важным изменениям, предлагаемым как часть бизнес-стратегии ИТ, и обеспечить наличие в организации решимости и возможностей для выполнения требуемых изменений.

5.3 Делегирование

5.3.1 Общие положения

Аспекты стратегического управления ИТ могут выполняться руководителями, если за ними закреплены соответствующие обязанности, переданными им руководящим органом вместе с делегированными полномочиями. [4.2 c)]

Руководящий орган обеспечивает выполнение целей организации с помощью руководителей организации. В зависимости от устава организации и в соответствии с применимыми законами и нормативными актами руководящий орган может делегировать отдельные полномочия одному или нескольким руководителям.

Стратегическое управление ИТ обычно осуществляется совместно руководящим органом и руководителями организации. Во многих организациях ответственность за использование ИТ распределяется между руководителями вместе с делегированием им полномочий по общему управлению организацией для достижения бизнес-целей, вместо того, чтобы явно ограничивать их ответственность только областью ИТ.

В принципе не существует ограничений, какие обязанности можно делегировать исполнительным руководителям, а какие обязанности остаются непосредственно за руководящим органом. На руководящем органе остается ответственность за эффективность и согласованность работы организации, даже когда отдельные функции по стратегическому и оперативному управлению, такие как принятие решений, делегированы. Сюда можно включить влияние на успехи или неудачи использования ИТ.

5.3.2 Делегирование полномочий руководящим органом

a) Руководящий орган может делегировать аспекты стратегического управления ИТ руководителям организации.

b) Для делегирования полномочий по стратегическому управлению ИТ, руководящий орган должен выполнить следующее:

- четко определить и согласовать обязанности и ограничения для принятия решений;
- сопоставить полномочия с подходящими ресурсами;
- обеспечить механизмы соответствия стратегиям и политикам и убедиться в том, что эффективность в достижении целей отслеживается и/или оценивается.

c) Руководящий орган должен обеспечить, что те, кому делегируются полномочия, обладают необходимыми компетенциями и что руководящий орган оставляет за собой соответствующий контроль за ключевыми решениями.

d) Руководящий орган должен определить и прояснить, какие решения требуют его непосредственного участия, а какие решения руководители могут принимать самостоятельно.

e) Руководящий орган должен обеспечить ясную формулировку в политиках управления степени, с которой ответственность за управление ИТ делегируется руководителям. В отношении ИТ руководящий орган обычно оставляет за собой решение следующих вопросов:

- утверждение целей, стратегий и политик использования ИТ;
- утверждение основных инвестиций в ИТ;
- контроль программ и проектов, наиболее сильно влияющих на бизнес;
- утверждение основных способов управления рисками, в частности, относящихся к безопасности и непрерывности бизнеса.

f) Руководящий орган должен обеспечить, чтобы целесообразность делегирования полномочий регулярно пересматривалась.

5.4 Обязанности руководителей

5.4.1 Общие положения

Руководители отвечают за достижение стратегических целей организации в соответствии со стратегиями и политиками использования ИТ, утвержденными руководящим органом. [4.2 d)]

В обязанности руководителей входит обеспечение достижения организацией необходимых результатов в рамках ограничений, установленных стратегиями и политиками ИТ, предусмотренных или утвержденных руководящим органом. Руководители отчитываются перед руководящим органом о полученных результатах. Обязанности руководителей, полномочия и подотчетность определяется руководящим органом. В некоторых юрисдикциях могут присутствовать специфические требования по отчетности для некоторых организационных ролей.

Руководители отвечают за реализацию стратегии и выполнение политики организации, также как за внедрение и контроль систем управления, необходимых для достижения целей, установленных руководящим органом.

5.4.2 Роль руководителей

a) Руководители должны обеспечивать достижение необходимых бизнес-результатов в рамках стратегий и политик использования ИТ, как установлено руководящим органом.

b) Руководители должны реализовывать стратегии, политики и системы менеджмента для достижения бизнес-целей, утвержденных руководящим органом. Эти стратегии и политики могут включать в себя:

- политики разработки и взаимодействия, руководства и стандарты для ИТ, основанные на принципах и политиках, предусмотренных или установленных руководящим органом;
- стратегическое планирование ИТ, как неотъемлемую часть стратегического планирования бизнеса при делегировании полномочий руководящим органом;
- внедрение механизмов управления спросом и предложением ИТ для поддержки инициатив изменения бизнеса организации;
- внедрение механизмов управления спросом и предложением ИТ для текущих бизнес операций;
- применение принципов управления рисками (интегрированных с системой управления рисками организации) к использованию ИТ;
- обеспечение управления инвестициями в ИТ как портфелем, включающим в себя всю деятельность, необходимую для увеличения ценности для бизнеса;
- контроль и оценка эффективности работы организации и ее соответствия требованиям и отчет о результатах руководящему органу.

c) Руководители должны принимать решения в соответствии с принятыми руководящим органом стратегиями и политиками организации.

5.5 Стратегическое управление и внутренний контроль

5.5.1 Общие положения

Для эффективного управления ИТ необходимо учредить эффективную систему внутреннего контроля как часть систем управления организацией. [4.2 e)]

Эффективное управление ИТ основывается на формировании эффективной системы внутреннего контроля как части формирования системы управления организацией для поддержки достижения бизнес-целей.

Руководители несут ответственность за оценку рисков в организации и внедрение соответствующей системы внутреннего контроля. Руководящий орган определяет политики внутреннего контроля, учитывая риск-аппетит организации, включая в себя требования законодательства. Управление рисками является ключевым элементом модели стратегического управления, так как необходимо учитывать риск при оценке, управлении и контроле.

5.5.2 Учреждение внутреннего контроля

a) Руководящий орган должен определить политики внутреннего контроля, учитывая риск-аппетит организации, включая в себя риск-аппетит использования ИТ и связанные с этим специфические требования.

b) Руководители должны внедрять системы управления, которые функционируют в рамках правил, как элемент системы стратегического управления, дополняющий принципы и практики стратегического управления и контроля в организации.

c) Специфические требования внутреннего контроля должны основываться на достижении бизнес-целей и внешних нормативных требованиях.

d) Контролирующие действия соответствующие уровню риска должны разрабатываться для снижения рисков, связанных с каждым процессом или проектом, которые могут повлиять на общую способность организации достичь бизнес-целей.

e) Система внутреннего контроля должна вытекать из системы стратегического управления:

- четкое распределение обязанностей, связанных с ИТ, в организации. Это включает в себя обязанности, ограничения ответственности, полномочия, подотчетность и структуру отчетов;
- для соответствующего выполнения обязанностей необходимо организовать обмен релевантной и достоверной информацией;
- управление рисками для определения и анализа ИТ рисков в отношении достижения бизнес-целей и выполнения политик организации, и обеспечение процедур управления рисками;
- непрерывный мониторинг системы внутреннего контроля наряду с регулярным пересмотром процедуры внутреннего контроля функционирования ИТ.

Приложение А
(справочное)

Принципы надлежащего стратегического управления ИТ

ИСО/МЭК 38500 описывает шесть принципов надлежащего стратегического управления ИТ. Эти принципы применимы к большинству компаний. В данном приложении приведен список этих принципов и их краткое описание. Для дополнительной информации следует обратиться к ИСО/МЭК 38500.

Принципы описывают предпочтительное поведение при принятии решений. Каждый принцип описывает, что должно случиться, но не описывает как, когда или кем принципы будут реализовываться, так как эти аспекты зависят от природы организации, использующей эти принципы. Руководящий орган должен требовать исполнения принципов.

Принцип 1. Ответственность

Лица и группы лиц в организации понимают и принимают ответственность в отношении, как спроса, так и предложения в области ИТ. Лица, ответственные за выполнение действий, обладают также полномочиями на осуществление таких действий.

Принцип 2. Стратегия

Стратегия развития организации учитывает текущие и будущие возможности ИТ, и стратегические планы по использованию ИТ соответствуют текущим и будущим потребностям стратегии бизнеса организации.

Принцип 3. Приобретение

Приобретение ИТ осуществляется на основе актуальных причин, надлежащего и непрерывного анализа, на основе четких и прозрачных решений. Поддерживается баланс выгод, возможностей, затрат и рисков, как в краткосрочной, так и в долгосрочной перспективе.

Принцип 4. Эффективность

ИТ соответствует цели поддержки деятельности организации, предоставляет услуги, уровень сервиса и качество которых должно соответствовать текущим и будущим потребностям бизнеса.

Принцип 5. Соответствие

ИТ соответствуют всем обязательным требованиям законодательства и нормативных актов. Политики и практики определены, внедрены и осуществляются.

Принцип 6. Поведение человека

Политики, практики и решения ИТ демонстрируют уважение к поведению людей, включая в себя текущие и будущие потребности всех лиц, задействованных в процессе.

Библиография

[1] ISO/IEC 38500, Information technology — Governance of IT for the organization
[2] ISO Guide 73, Risk management — Vocabulary
[3] OECD Principles of Corporate Governance, OECD, 1999 and 2004
[4] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary

УДК 004:006.354 ОКС 35.020

Ключевые слова: информационные технологии, стратегическое управление ИТ

БЗ 11—2019/36

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *М.С. Кабашова*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 21.10.2019. Подписано в печать 15.11.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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