ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 30121— 2017

Информационные технологии

КОНЦЕПЦИЯ УПРАВЛЕНИЯ РИСКАМИ, СВЯЗАННЫМИ С ПРОВЕДЕНИЕМ СУДЕБНОЙ ЭКСПЕРТИЗЫ СВИДЕТЕЛЬСТВ, ПРЕДСТАВЛЕННЫХ В ЦИФРОВОЙ ФОРМЕ

(ISO/IEC 30121:2015, 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 10 октября 2017 г. № 1382-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 30121:2015 «Информационные технологии. Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме» (ISO/IEC 30121:2015 «Information technology — Governance of digital forensic risk framework», IDT).

ISO/IEC 30121 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).

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

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

Организации разных типов сталкиваются с внутренними и внешними факторами и воздействием, которые могут привести к возникновению ситуаций, требующих проведения судебной экспертизы и получения свидетельств, представленных в цифровой форме, с использованием информационных технологий (ИТ) и связанных с ними информационных систем (ИС). Необходимость проведения судебной экспертизы может возникнуть в результате неизвестных, внеплановых или непредвиденных событий либо в процессе запланированного разбирательства против сотрудников, конкурентов или поставщиков услуг. Значимость риска, связанного с проведением судебной экспертизы, зависит от уровня риска и отношения к нему организации. Отношение организации к риску будет отражаться в критерии риска. Поскольку свидетельства, представленные в цифровой форме, как правило, будут получены и представлены суду, организациям следует заблаговременно готовиться к подобным ситуациям.

Настоящий стандарт описывает последовательную стратегическую подготовку организации к судебной экспертизе свидетельств, представленных в цифровой форме. Готовность организации к судебной экспертизе означает, что в ней проведена соответствующая и релевантная стратегическая подготовка к событиям, которые могут привести к судебному расследованию. Оно может быть вызвано неизбежными нарушениями безопасности, мошенничеством и угрозой репутации. Во всех случаях использование ИТ должно стратегически максимизировать эффективность поиска свидетельств, их доступность, а также оптимизировать связанные с этим затраты.

Руководящий орган должен отвечать за выработку стратегического направления во всех важных для организации областях. Руководящий орган должен следовать принципам лучших практик, которые обеспечивают общее руководство по вопросам достоверности и соответствия. Эти принципы могут содержаться в юридических предписаниях, стандартах, требованиях соблюдения общественных и культурных норм. В настоящем стандарте в качестве лучших практик управления ИТ (раздел 4) используются принципы ИСО/МЭК 38500.

Эти принципы должны быть реализованы. Задачи управления включают в себя оценку предложений и планов, отслеживание их выполнения и соответствия требованиям, выработку стратегии и политик. Заинтересованные лица организации могут предоставить предписание для руководства, однако окончательную ответственность за риск несет руководящий орган. Концепция управления рисками, связанными с проведением судебной экспертизы свидетельств, представленных в цифровой форме, устанавливается ответственными за риск лицами путем выполнения действий, соответствующих стратегическому направлению развития организации. Следовательно, стратегической целью организации является реализация принципов и обеспечение надлежащей подготовки к проведению судебной экспертизы свидетельств, представленных в цифровой форме (раздел 5).

Стратегические процессы должны обеспечить направление действий для руководителей и топ-менеджеров в соответствии с выбранной концепцией. Стратегические процессы должны выбираться таким образом, чтобы обеспечить адекватную область действий и быть принципиально архивируемыми, открытыми, производительными и соответствующими критерию риска (раздел 6).

Для измерения соответствия целям, вытекающим из установленных принципов, используются ключевые показатели достижения целей (KGI), для измерения выполнения стратегических задач, вытекающих из стратегии, — ключевые показатели производительности (KPI), а расхождение между KGI и KPI отражает ключевой показатель бизнеса организации (KBI) (раздел 7).

Настоящий стандарт следует использовать вместе со словарем, приведенным в Руководстве ИСО 73:2009, с ИСО/МЭК ТО 38502 «Информационные технологии. Управление ИТ. Схема и модель», а также ИСО/МЭК 38500 «Информационные технологии. Управление ИТ в организации».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

КОНЦЕПЦИЯ УПРАВЛЕНИЯ РИСКАМИ, СВЯЗАННЫМИ С ПРОВЕДЕНИЕМ СУДЕБНОЙ ЭКСПЕРТИЗЫ СВИДЕТЕЛЬСТВ, ПРЕДСТАВЛЕННЫХ В ЦИФРОВОЙ ФОРМЕ

Information technology. Governance of digital forensic risk framework

Дата введения — 2018—09—01

1 Область применения

Настоящий стандарт описывает концепцию, помогающую руководящим органам организаций (включая владельцев, членов правления, директоров, партнеров, высшее руководство и т. д.), наилучшим образом заблаговременно подготовить организацию к проведению судебных экспертиз свидетельств, представленных в цифровой форме, до того, как они потребуются. Настоящий стандарт может быть применим при разработке стратегических процессов (и решений), связанных с хранением и доступностью данных, а также экономической эффективностью свидетельств, представленных в цифровой форме. Настоящий стандарт применим к организациям разных типов и размеров. Структура настоящего стандарта приведена в приложении А.

2 Нормативные ссылки

В настоящем стандарте применены следующие нормативные ссылки. Для датированных документов используются только указанные издания. Для недатированных документов используются последние издания с учетом внесенных в них изменений.

ISO/IEC 38500 Information technology — Governance of IT for the organization (Информационные технологии. Управление ИТ в организации)

ISO Guide 73:2009 Risk management — Vocabulary (Управление рисками. Словарь)

3 Термины и определения

В настоящем стандарте применены термины, определенные в ИСО/МЭК 38500, Руководстве ИСО 73:2009, а также следующие термины с соответствующими определениями:

3.1

свидетельства, представленные в цифровой форме (digital evidence): Информация или данные, хранящиеся или переданные в виде двоичного кода, которые могут быть использованы в качестве доказательства.

[ИСО/МЭК 27037:2012, статья 3.5]

3.2

руководящий орган (governing body): Человек или группа людей, которые несут ответственность перед заинтересованными лицами за работоспособность организации и соответствие требованиям.

[ИСО/МЭК ТО 38502:2014, статья 2.9]

Издание официальное

3.3 **судебная экспертиза свидетельств, представленных в цифровой форме** (digital forensics): Использование научных знаний, технологий и методик при исследовании свидетельств, представленных в цифровой форме, для целей судопроизводства.

3.4 **стратегический риск** (strategic risk): Влияние неопределенности на достижение целей.

4 Принципы

4.1 Ответственность

Лица и группы лиц в организации должны понимать и брать на себя ответственность в отношении как предоставления, так и требования свидетельств, представленных в цифровой форме. Лица, ответственные за экспертизу, должны быть независимы, а также обладать необходимыми компетенциями и полномочиями на выполнение таких действий.

4.2 Стратегия

При разработке стратегии организации следует принимать во внимание текущее и будущее хранение и доступность данных, а также экономическую эффективность свидетельств, представленных в цифровой форме; стратегическое планирование должно соответствовать текущим требованиям организации.

4.3 Приобретение

Приобретение ИТ-активов должно поддерживаться стратегией организации на основе надлежащего и непрерывного анализа, с четким и прозрачным принятием решений. Должен существовать необходимый баланс между выгодами, возможностями, затратами и рисками как в краткосрочной, так и в долгосрочной перспективе.

4.4 Эффективность

ИТ должно соответствовать целям поддержки организации, предоставления услуг, обеспечения необходимого уровня и качества обслуживания для удовлетворения текущих и будущих потребностей организации в отношении свидетельств, представленных в цифровой форме.

4.5 Соответствие требованиям

ИТ-активы должны отвечать всем обязательным законодательным нормам и требованиям. Методики и политики должны быть четко определены, внедрены и применимы в соответствии с принятыми в организации критериями риска.

4.6 Поведение человека

Политики, методики и решения в сфере судебной экспертизы свидетельств, представленных в цифровой форме, должны быть основаны на уважении к людям, их поведению, включая существующие и будущие потребности всех людей, задействованных в процессах организации.

5 Концепция

5.1 Полномочия заинтересованных лиц

Руководящий орган, образованный для защиты интересов заинтересованных лиц, должен обладать достаточными полномочиями для выбора стратегического направления развития организации и определения ее функциональных возможностей.

5.2 Постановка задачи

Цикл работы руководящего органа должен соответствовать этапам оценки, выбора направления и отслеживания и способствовать принятию стратегической политики, стратегического планирования и стратегических возможностей.

5.3 Оценка

Руководящий орган должен изучать и оценивать текущие и будущие потребности в свидетельствах, представленных в цифровой форме, в том числе стратегии, предложения, планы и договоренно-

сти по поставкам (внутренние, внешние или и те, и другие). При оценке использования ИТ должны быть учтены требования предоставления свидетельств, представленных в цифровой форме, и организации процессов судебной экспертизы.

5.4 Направление

Руководящий орган должен распределять ответственность за прямую подготовку и реализацию стратегий, планов и политик, а также контролировать их выполнение. Планы должны определять стратегическое направление для свидетельств, представленных в цифровой форме, операционной деятельности и возможностей ИТ. Руководящие органы должны поощрять культуру эффективного управления ИТ в своих организациях, требуя от руководителей предоставления своевременной информации, соблюдения стратегических направлений в соответствии с критерием риска.

5.5 Отслеживание

Используя соответствующие измерительные системы, руководящий орган должен отслеживать эффективность ИТ-систем и их соответствие свидетельствам, представленным в цифровой форме. Следует постоянно следить за тем, чтобы работа велась в соответствии со стратегическими планами, а уровни риска находились в пределах установленного для организации критерия риска. Руководящий орган должен нести ответственность за эффективное, действенное и приемлемое использование ИТ для получения свидетельств, представленных в цифровой форме, в организации; эта ответственность не должна быть делегирована.

6 Процессы

6.1 Стратегия архивации

Организация должна определять целостное архивное хранение информационных активов. Процессы архивации должны быть структурированными, полными, эффективными, безопасными и обеспечивать целостность данных.

6.2 Стратегия обнаружения

Организация должна устанавливать эффективные и действенные средства поиска информации. Точный и своевременный доступ к организационной информации критичен для принятия решений и предоставления доказательств.

6.3 Стратегия разглашения

Организация должна устанавливать критерий для защиты и разглашения информации. Для любой оценки рисков, связанных с проведением судебной экспертизы свидетельств, представленных в цифровой форме, с которыми сталкивается организация, должен быть применен критерий, позволяющий определить допустимость уровня риска и потребность в принятии дальнейшего стратегического риска. Разглашаемая информация должна сохраняться с возможностью проведения аудита.

6.4 Стратегия реализации возможностей судебной экспертизы свидетельств, представленных в цифровой форме

Организация должна формировать политики и планы таким образом, чтобы обеспечить сохранность свидетельств, представленных в цифровой форме, и хранение и/или доступ к компетенциям судебной экспертизы свидетельств, представленных в цифровой форме. Организация должна поддерживать процессы, обеспечивающие объективность расследований, независимость экспертов и доказательную силу информации, представленной в виде двоичного кода.

6.5 Стратегия управления рисками и соответствием

Организация должна выбирать решения о принятии стратегических рисков, основанные на применении критерия риска к свидетельствам, представленным в цифровой форме. Руководящий орган должен гарантировать, что уровень риска находится в соответствии с установленным организацией критерием риска.

7 Метрики

7.1 Основные положения

Организация должна измерять важные атрибуты объектов для оценки предложений и планов, отслеживания производительности и соответствия требованиям, выработки стратегии и политик. Отчеты должны обеспечивать руководящий орган организации информацией, на основе которой должны приниматься обоснованные решения.

7.2 Ключевые показатели достижения целей

Ключевые показатели достижения целей (KGI) отражают значение атрибутов достижения целей. С помощью KGI можно отслеживать достижение ключевых целей.

7.3 Ключевые показатели производительности

Ключевые показатели производительности (KPI) отражают значение атрибутов выполнения задач. С помощью KPI можно отслеживать выполнение процессов.

7.4 Ключевые показатели бизнеса

Ключевые показатели бизнеса (KBI) отражают расхождение между ключевыми показателями достижения целей (KGI) и ключевыми показателями производительности (KPI). С помощью KBI можно отслеживать организационный прогресс.

Приложение А
(справочное)

Структура настоящего стандарта

Структура настоящего стандарта приведена на рисунке А.1.

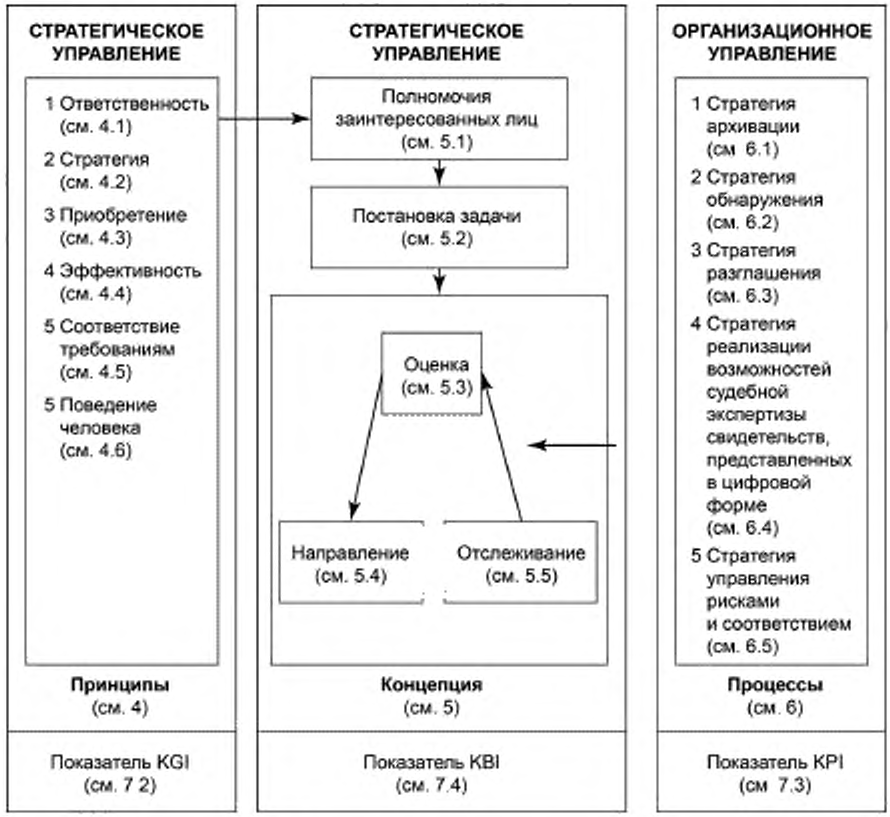

Рисунок А.1 — Структура настоящего стандарта

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 38500:2015	—	*
ISO Guide 73:2009	IDT	ГОСТ Р 51897—2011/ Руководство ИСО 73:2009 «Менеджмент риска. Термины и определения»

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] ISO 31000:2009, Risk management — Principles and guidelines
[2] ISO 31010:2009, Risk Management — Risk assessment techniques
[3] ISO/IEC TR 38502:2014, Information technology — Governance of IT — Framework and model

УДК 004:006.034 ОКС 35.080 IDT

Ключевые слова: управление рисками, свидетельства, представленные в цифровой форме, судебная экспертиза свидетельств, представленных в цифровой форме, стратегический риск, ключевые показатели бизнеса (KBI), ключевые показатели производительности (KPI), ключевые показатели достижения целей (KGI)

БЗ 7—2017/12

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *А.А. Ворониной*

Сдано в набор 11.10.2017. Подписано в печать 24.10.2017 Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,28. Тираж 21 экз. Зак. 2069

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