Утвержден и введен в действие
Приказом Федерального агентства
по техническому регулированию
и метрологии
от 20 июля 2017 г. N 731-ст

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИЯ И ДОКУМЕНТАЦИЯ

ОЦЕНКА РИСКОВ ДЛЯ ДОКУМЕНТНЫХ ПРОЦЕССОВ И СИСТЕМ

Information and documentation. Risk assessment for records processes and systems

(ISO/TR 18128:2014, IDT)

ГОСТ Р 57551-2017/ISO/TR 18128:2014

ОКС 37.080:
25.040.40

Дата введения
1 июля 2019 года

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью "ЭОС Тех" на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 459 "Информационная поддержка жизненного цикла изделий"

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 июля 2017 г. N 731-ст

4 Настоящий стандарт идентичен международному стандарту ISO/TR 18128:2014 "Информация и документация. Оценка рисков для документных процессов и систем" (ISO/TR 18128:2014 "Information and documentation - Risk assessment for records processes and systems", IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. N 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)

Вступление

Международная организация по стандартизации ИСО (International Organization for Standardization, ISO) является всемирным объединением национальных органов по стандартизации - членов ИСО. Работа по подготовке международных стандартов обычно проводится техническими комитетами ИСО. Каждый член ИСО, заинтересованный в вопросе, для проработки которого был создан технический комитет, имеет право быть представленным в этом комитете. Международные правительственные и неправительственные организации, имеющие партнерские связи с ИСО, также принимают участие в этой работе. ИСО тесно сотрудничает с Международной электротехнической комиссией МЭК (International Electrotechnical Commission, IEC) по всем вопросам стандартизации в области электротехники.

Международные стандарты разрабатываются и в дальнейшем поддерживаются в соответствии с правилами, установленными в части 1 директив ИСО/МЭК. Следует, в частности, иметь в виду различные критерии, соответствие которым необходимо для утверждения документов ИСО разных типов. Технический отчет ИСО/ТО 18128:2014 был разработан в соответствии с правилами редакционной работы, установленными частью 2 директив ИСО/МЭК <1>.

<1> См. www.iso.org/directives.

Следует принять во внимание, что некоторые элементы данного документа могут подпадать под действие патентного права. ИСО и МЭК не несут ответственность за идентификацию соответствующих патентных прав. Сведения о выявленных в ходе разработки технического отчета ИСО/ТО 18128:2014 патентных правах содержатся во введении и/или в перечне ИСО полученных патентных деклараций <2>.

<2> См. www.iso.org/patents.

Все встречающиеся в данном документе торговые наименования представляют собой сведения, включенные для удобства пользователей, и их упоминание не означает официальной поддержки соответствующих продуктов со стороны ИСО.

Разъяснения принятых в ИСО трактовок специфических терминов и выражений, относящихся к оценке соответствия, а также информацию о приверженности ИСО принципам ВТО в части борьбы с техническими барьерами для торговли (Technical Barriers to Trade, TBT) можно найти на веб-сайте ИСО по адресу http://www.iso.org/iso/home/standards_development/resources-for-technical-work/foreword.htm.

Технический отчет ИСО/ТО 18128:2014 был разработан Техническим подкомитетом ПК 11 "Управление документами и архивами" Технического комитета ИСО/ТК 46 "Информация и документация" (ISO/TC 46/SC 11 "Archives/records management", ISO/TC 46 "Information and documentation").

Введение

Все организации идентифицируют угрожающие их успешному функционированию риски и управляют ими. Специалисты организации по управлению документами несут ответственность за идентификацию и управление рисками, относящимися к документным процессам и системам.

Настоящий стандарт должен помочь специалистам по управлению документами и ответственным за документы в своих организациях сотрудникам оценивать риски, связанные с документными процессами и системами.

Примечание - Под "системой" понимается любое деловое программное приложение, в котором создаются и хранятся документы.

Данная задача отличается от более общей задачи идентификации и оценки деловых рисков организации, где создание и хранение адекватных документов является одним из стратегических способов реагирования. Решения о необходимости создания документов в качестве реакции на риски для основной деятельности являются деловыми решениями, которые должны приниматься с учетом результатов анализа требований и потребностей организации в документах, проводимого совместно специалистами по управлению документами и представителями деловых подразделений. Настоящий стандарт исходит из того, что организация создала отражающие ее деловую деятельность документы с тем, чтобы удовлетворить потребности оперативной деятельности и иные нужды, и, по крайней мере, внедрила минимальный набор мер, обеспечивающих систематическое управление документами и контроль над ними.

Последствием рисковых событий для документных процессов и систем является утрата или повреждение документов, которые в результате становятся непригодными для использования, утрачивают надежность, аутентичность, полноту и/или неизменность, и могут поэтому не удовлетворять потребностям организации.

Настоящий стандарт содержит рекомендации и примеры, основанные на общих принципах менеджмента риска, установленных ИСО 31000 (см. рисунок 1), которые применены в отношении рисков, связанных с документными процессами и системами. Стандарт охватывает следующие вопросы:

a) идентификация рисков,

b) анализ риска,

c) сравнительная оценка риска.

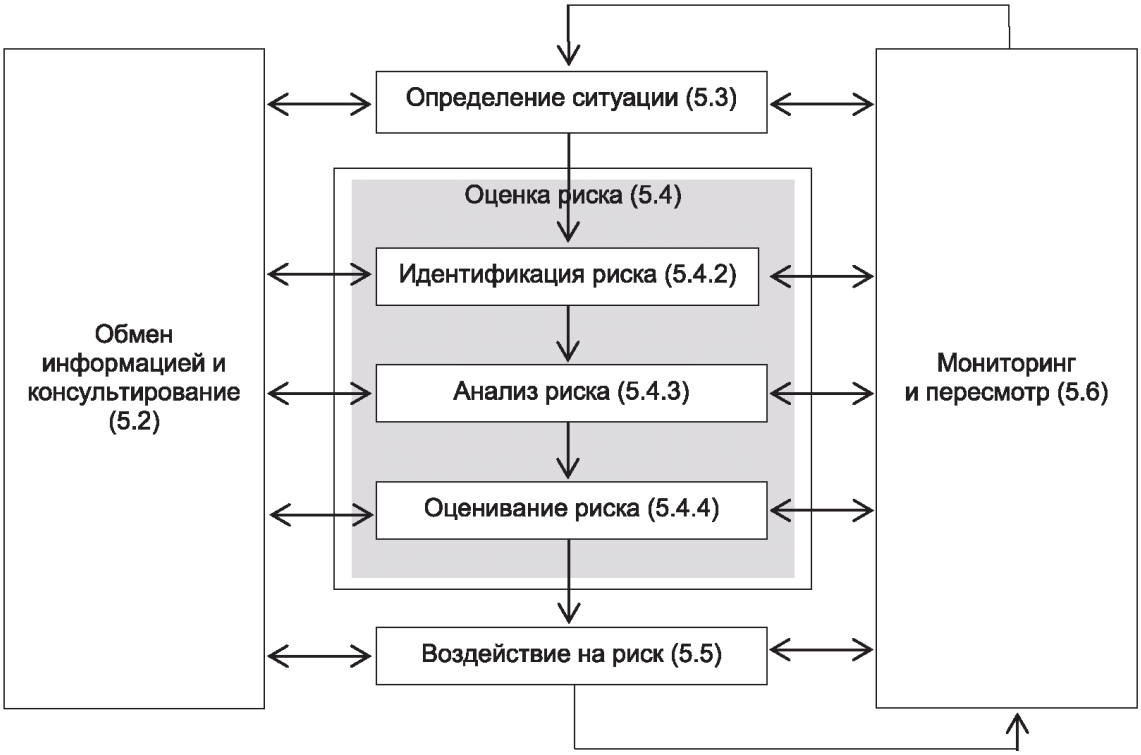

Рисунок 1 - Процесс менеджмента риска

Примечание - Рисунок 1 взят из ИСО 31000:2009. Приведенная на нем нумерация разделов относится к тексту указанного стандарта.

Результаты анализа риска для документных процессов и систем следует включать в общую систему управления рисками организации. В результате организация будет лучше контролировать свои документы и их качество в плане использования в деловых целях.

Раздел 5 содержит всесторонний перечень областей неопределенности, связанных с документными процессами и системами, предназначенный для идентификации рисков.

Раздел 6 содержит руководство по определению последствий и вероятностей идентифицированных рисковых событий с учетом наличия (или отсутствия) и эффективности применяемых мер и средств контроля и управления.

Раздел 7 содержит руководство по определению значимости уровня и типа идентифицированных рисков.

Стандарт не затрагивает вопросы воздействия на риски. По завершении оценки рисков, связанных с документными процессами и системами, эти риски документируются и соответствующие сведения передаются в подразделение (службу) организации, занимающееся менеджментом риска. Реагирование на оцененные риски осуществляется в рамках общей программы управления рисками организации. Приоритет, установленный оцененным рискам специалистом по управлению документами, впоследствии учитывается при принятии организацией решений об управлении этими рисками.

1 Область применения

Настоящий стандарт должен помочь организациям в оценке рисков для документных

процессов и систем, для обеспечения того, чтобы документы удовлетворяли выявленным потребностям деятельности до тех пор, пока в этом сохраняется необходимость.

Настоящий стандарт:

a) устанавливает метод анализа, проводимого с целью идентификации (выявления) рисков, связанных с документными процессами и системами;

b) описывает метод анализа потенциальных последствий неблагоприятных событий для документных процессов и систем;

c) содержит рекомендации по проведению оценки рисков, связанных с документными процессами и системами, а также

d) содержит рекомендации по документированию выявленных и оцененных рисков, в рамках подготовки к смягчению или устранению этих рисков.

В настоящем стандарте не рассматриваются риски для деятельности организации общего характера, которые могут быть смягчены, в том числе, путем создания документов.

Настоящий стандарт может быть использован любыми организациями, вне зависимости от их размера, характера деятельности и сложности их функций и структуры. Перечисленные факторы, а также предписывающий создание документов и контроль над ними режим законодательно-нормативного регулирования, в условиях которого организация осуществляет свою деятельность, принимаются во внимание при идентификации и оценке рисков, связанных с документами и документными системами.

При установлении границ ответственности организации следует учитывать сложную систему взаимоотношений с другими организациями и внешними и внутренними заинтересованными сторонами, в том числе партнерские отношения и договорные обязательства, касающиеся цепочек поставок и передачи на аутсорсинг ряда функций, которые являются характерной особенностью деятельности современных государственных и коммерческих организаций. Установление границ ответственности организации является первым шагом в определении объема и содержания проекта оценки связанных с документами рисков.

В настоящем стандарте вопрос воздействия на риски (смягчения рисков) непосредственно не рассматривается, поскольку соответствующие методы являются специфическими для каждой организации.

Стандарт может быть использован специалистами по управлению документами, лицами, несущими в своих организациях ответственность за документы, а также аудиторами и руководителями, отвечающими в организациях за программы менеджмента риска.

2 Нормативные ссылки

Настоящий стандарт содержит ссылки нормативного характера на перечисленные ниже документы, которые (полностью или частично) необходимы для его применения. Для датированных ссылок применима только та версия, которая упомянута в тексте. В случае недатированных ссылок необходимо использовать последнюю редакцию документа (включая опубликованные поправки).

ISO 30300:2011 Information and documentation - Management systems for records - Fundamentals and vocabulary (Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Системы управления документами.

Основные положения и словарь)

ISO Guide 73:2009 Risk management - Vocabulary (Менеджмент риска. Термины и определения)

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 Термины, относящиеся к риску

3.1.1 **риск** (risk): Следствие влияния неопределенности на достижение поставленных целей.

Примечание 1 - Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

Примечание 2 - Неопределенность - это состояние полной или частичной нехватки информации, знаний и понимания события, его последствий и/или их вероятности.

Примечание 3 - Риск часто характеризуют путем описания возможного события (Руководство ИСО 73:2009, 3.5.1.3) и его последствий (Руководство ИСО 73:2009, 3.6.1.3) или их сочетания.

Примечание 4 - Риск часто описывают в виде комбинации последствий возможного события (в том числе изменения обстоятельств) и соответствующей вероятности наступления этого события (Руководство ИСО 73:2009, 3.6.1.1).

[Руководство ИСО 73:2009, 1.1]

3.2 Термины, относящиеся к документам

3.2.1 **документная система, система управления документами** (records system): Информационная система, обеспечивающая захват документов, а также управление документами и доступ к ним во времени.

Примечание 1 - К числу документных систем могут быть отнесены создающие и хранящие документы деловые приложения и системы.

[ИСО 30300-2011, 3.4.4]

3.2.2 **документные процессы, процессы управления документами** (records processes): Совокупности взаимосвязанных или взаимодействующих видов деятельности, с использованием которых организация создает, контролирует, использует, уничтожает либо передает на архивное хранение свои документы.

4 Критерии оценки риска для организации

4.1 Оценка риска

Оценка рисков для документных процессов и систем должна включаться в общий процесс управления рисками организации, где таковой существует. В этом случае специалисты по управлению документами должны учитывать внешние и внутренние обстоятельства и условия, в

которых организация осуществляет свою деятельность (контекст), а также контекст самого процесса менеджмента риска, в том числе следующие факторы:

a) роли и обязанности: Должна быть определена роль специалистов по управлению документами в оценке рисков, связанных с документными процессами и системами;

b) охват и масштабы деятельности по оценке рисков: Во избежание избыточности и конфликтов, а также для создания условий для применения комплексного подхода к оценке рисков, связанных, в том числе, с документами, следует явным образом определить взаимоотношения с другими областями оценки риска, такими как информационная безопасность;

c) методология: При использовании имеющихся инструментов для оценки рисков и при подготовке отчетов перед уполномоченным лицом или службой следует использовать стандартную методологию оценки риска;

d) критерии риска: В случае, когда в организации используются общие критерии риска, следует оценивать связанные с документными процессами и системами риски на основе этих критериев.

Если в организации отсутствует общий процесс управления рисками, то специалистам по управлению документами до начала процесса оценки следует установить критерии риска, применимые к документным процессам и системам.

4.2 Критерии риска

Критерии должны быть основаны на нормативно-правовых требованиях юрисдикции, в рамках которой действует организация, и включать в себя следующее:

a) природу и типы принимаемых во внимание последствий и способы их измерения;

b) способы отражения вероятности событий;

c) подход к определению уровня риска;

d) критерии, на основе которых будет приниматься решение о необходимости воздействия на риск (т.е. об устранении или снижении риска);

e) критерии для принятия решения о приемлемости и/или допустимости риска;

f) будут ли учитываться возможные комбинации рисков, и если да, то каким образом.

Что касается природы и типов последствий, которые должны быть охвачены при оценке риска для документных процессов и систем, то существует общая отправная точка, применимая во всех организациях. Аутентичные, надежные, целостные документы, пригодные к использованию в течение всего периода времени, пока в них сохраняется необходимость, будут способны удовлетворить потребности организации. Риски идентифицируются, исходя из их возможности нанести ущерб этим общим свойствам документов, в результате чего документы могут уже не соответствовать тем целям, ради которых они были созданы.

Вопросы анализа вероятности и частоты событий в рамках оценки рисков обсуждаются в 6.2.

Критерии количественной оценки рисков, в том числе критерии, на основе которых будут

приниматься решения о приемлемости риска или необходимости его снижения, включают размер и охват документных систем организации, количество пользователей этих систем, а также способ применения таких систем в оперативной деятельности организации.

Аналогичным образом критерии количественной оценки рисков для документных процессов должны включать частоту выполнения процесса, количество систем в которых он выполняется, его относительную важность для создания и управления документами, возможности для мониторинга процессов, а также потенциальные возможности для полного устранения или смягчения неблагоприятных последствий.

4.3 Определение приоритетов

Как правило, организация должна определить, какие документы являются ключевыми для ее деятельности, а также придаваемый им уровень значимости. Это деловые решения, основанные на рекомендациях как специалистов по управлению документами, так и представителей деловых подразделений.

Приоритет, установленный для отдельных документов, их массивов, для документных процессов или конкретных документных систем, также может приниматься во внимание в связи с реагированием на крупные чрезвычайные происшествия, затрагивающие все или многие деловые операции. Например, определенные документы могут потребоваться сразу же после стихийного бедствия, такие как адреса и телефоны экстренных служб, сведения о проходе лиц на территорию объекта, контактные данные групп реагирования на чрезвычайные ситуации, контактные данные страховых компаний и конкретные условия страхования. Кроме того, при планировании мер по обеспечению непрерывности своей деятельности организациям следует определить, какие деловые функции должны быть восстановлены в первую очередь и какие документы для этого понадобятся.

Особое внимание следует уделить ситуациям, в которых документы, отнесенные к числу ключевых для оперативной деятельности, подвергаются комбинации рисков.

5 Идентификация риска

5.1 Общие положения

Идентификация риска проводится по следующим направлениям: анализируются контекст деятельности, системы, а также процессы, используемые при создании и управлении документами организации.

Под внешним контекстом деятельности организации понимается совокупность неподконтрольных ей общественно-политических, макроэкономических, технологических, а также физических и экологических факторов, оказывающих влияние на ее деятельность и учитываемых при определении связанных с документами требований и потребностей организации. Частью внешнего контекста являются внешние заинтересованные стороны, имеющие конкретные интересы, связанные с деятельностью организации.

Существует также внутренний контекст деятельности организации, под которым понимается совокупность внутренних факторов, неподконтрольных ответственным за документные процессы и системы специалистам по управлению документами. Внутренний контекст включает в себя такие факторы, как структура и финансы организации, применяемые ею технологии, ресурсное обеспечение деятельности (кадры и бюджеты), а также культура организации, которые влияют на политики и практику управления документами.

Потенциально возможные события с не вполне предсказуемыми последствиями могут быть

как внешними, так и внутренними по отношению к организации.

Различные подразделения организации могут иметь разные точки зрения на неопределенности, связанные с последствиями изменений внешнего контекста (см. рисунок 2). Кроме того, следует иметь в виду, что любые изменения открывают новые возможности, последствия которых могут быть и положительными.

Рисунок 2 - Множественность слоев контекста для документов и документных процессов организации

Цель идентификации риска заключается в выяснении того, что может произойти и какие ситуации могут возникнуть, чтобы это в итоге повлияло на способность документов удовлетворять потребности организации.

Процесс идентификации риска включает в себя выявление причин и источников риска, событий, ситуаций или обстоятельств, способных существенно повлиять на достижение организацией своих целей, а также выяснение природы такого влияния. Сопоставление основных методов дано в приложении В к МЭК 31010.

Выявленные риски должны быть задокументированы в реестре рисков. Это может быть как специальный реестр рисков для документов, так и общий реестр рисков организации. Соответствующий пример приведен в приложении А.

Примечание - В приложении В к настоящему стандарту приведен пример построенного в соответствии со структурой раздела 5 списка контрольных вопросов (контрольного списка),

который организация может использовать для систематической идентификации рисков для документных процессов и систем.

5.2 Контекст деятельности организации: внешние факторы

5.2.1 Области неопределенности: изменения в общественно-политическом контексте

Изменения в политическом и общественном климате, как на национальном, так и на международном уровне, могут повлиять на отношение общества к поведению государственных органов и коммерческих организаций. Это может привести к изменениям в законодательстве и нормативной базе, которые повлияют на деятельность организаций и, как следствие, на их требования к документам.

Примерами областей, в которых изменение общественного отношения может повлиять на требования к документам, являются обеспечение национальной безопасности, доступ к государственной и корпоративной информации, неприкосновенность частной жизни и защита персональных данных, права интеллектуальной собственности, а также обязанности корпораций по раскрытию информации об их деятельности. В более общем плане примерами областей неопределенности являются:

a) законодательно-нормативные изменения, влияющие на требования организаций к документам;

b) изменения в государственной политике, влияющие на документы, документные процессы и системы организации;

c) новые стандарты и кодексы практики, влияющие на документы, документные процессы и системы организации;

d) изменение спроса на услуги в области управления документами;

e) изменение ожиданий заинтересованных сторон;

f) изменение репутации либо доверия к способности организации предоставлять свои услуги.

5.2.2 Области неопределенности: макроэкономическая и технологическая среда

Изменения в макроэкономической, деловой и производственной средах, а также в информационных технологиях сильно влияют на конкуренцию и потребительский спрос. Изменения могут проходить постепенно и непрерывно, но могут быть и результатом кризисов. Они также представляют собой области неопределенности, с которыми могут быть связаны, в том числе и позитивные возможности.

Примеры областей неопределенности, вытекающих из подобных изменений в макроэкономической и деловой среде, включают в себя следующее:

a) изменения в собственности и/или выручке организации, влияющие на приоритеты в сфере управления, включая управление документами;

b) изменения в целях, функциях и оперативной деятельности организации, приводящие к изменению требований к документам;

c) повышение активности регулирующих органов, приводящее к росту числа внешних

запросов на представление документов;

d) увеличение числа судебных разбирательств, приводящее к росту числа запросов на представление документов;

e) внедрение и широкое распространение новых технологий в масштабах всего общества;

Пример - Использование социальных сетей и мобильных компьютерных устройств для ведения деятельности.

f) изменения на рынке или в клиентской базе организации.

Эти изменения находят свое отражение в организационных переменах, которые рассматриваются ниже (см. 5.3.1).

5.2.3 Области неопределенности: физическая среда и инфраструктура

Возможность крупномасштабных природных и техногенных катастроф, способных повлиять на деятельность организации в целом, является одной из главных областей неопределенности, требующей идентификации и оценки. Потенциальный ущерб от таких катастроф включает как непосредственное воздействие на документы и их хранилища, так и менее прямолинейное влияние вследствие утраты услуг, от которых организация зависит, таких как водо- и электроснабжение и ряд других. В число областей неопределенности входят следующие:

a) региональные или местные разрушительные или нарушающие нормальную деятельность природные явления, такие как землетрясения, ураганы/циклоны, цунами, наводнения, пожары, мощные штормы и длительная засуха;

b) возможность серьезных структурных повреждений и перебоев с оказанием услуг в помещениях или в непосредственной близости от местоположения организации вследствие военных действий или террористических актов;

c) различные перебои в организации с энергоснабжением, подачей воды, вывозом отходов, с информационными технологиями, оказанием транспортных услуг и иных основных коммунальных услуг и сервисов.

5.2.4 Области неопределенности: внешние угрозы безопасности

Идентификация риска должна охватывать враждебные внешние угрозы безопасности, потенциальное воздействие которых может варьироваться от повреждения помещений и помех оказанию услуг до несанкционированного доступа к системам, в том числе документным. Примерами внешних угроз могут быть:

a) несанкционированное внешнее вторжение/доступ в документные системы и внесение несанкционированных изменений в документы;

b) оставшаяся незамеченной компрометация системы безопасности или использование неконтролируемой уязвимости, приводящее к деградации информации;

Пример - Атака с использованием шпионского или вредоносного программного обеспечения либо уязвимостей, связанных с неисправленными слабыми сторонами и нарушениями защиты программного обеспечения.

c) физическое вторжение в хранилище документов или в зону размещения

ИТ-оборудования;

d) атака "отказ в обслуживании" (DDOS-атака) и иные преднамеренные атаки на интернет-услуги;

e) физический вандализм;

f) утрата услуг третьих сторон, от которых зависят документные системы.

Примечание - Оценка риска является неотъемлемым элементом внедрения международных стандартов серии ИСО/МЭК 27000 в области информационной безопасности. В этих стандартах подробно рассматриваются области неопределенности, связанные с информационной безопасностью.

5.3 Контекст деятельности организации: внутренние факторы

5.3.1 Области неопределенности: организационные изменения

Влияющие на организацию управленческие решения, такие как решения о слиянии компаний, о поглощении другой компании, о прочих приобретениях, реструктуризациях, сокращениях, передаче функций на аутсорсинг либо переводе в оффшоры представляют собой значительную область неопределенности во внутреннем контексте организации. Подобные решения будут влиять на документные процессы и системы, например:

a) изменение прав собственности на документы и документные системы, и последующая передача документов в организацию и из нее;

b) изменение прав собственности на документы и документные системы, приводящее к вынужденной миграции документов или к объединению систем;

c) соглашения о доступе к документным системам, обеспечивающие право непрерывного доступа к документам после их передачи и миграции;

d) наследование ответственности за документы и документные системы в отсутствие адекватной документации;

e) утрата персонала или корпоративной памяти, отражающиеся на имеющихся у организации знаниях о текущих документах и системах, в том числе о процедурах извлечения и использования документов, и на знаниях о более старых документах, унаследованных через организационные изменения;

f) прекращение использования документов и документных систем, особенно унаследованных систем, за которые никто не несет ответственность;

g) изменение условий в договорах с третьими сторонами об оказании услуг;

h) введение новых или модификация существующих внутренних политик организации, влияющих на документные системы и процессы;

i) наличие политик и процедур, которые не были своевременно пересмотрены и обновлены и стали неприменимыми либо стали несогласованными или противоречивыми в результате организационных изменений;

j) изменения в кадровом составе организации, которые могут повлиять на распределение

ответственности за документы;

k) изменения в кадровой политике, в финансировании и возможностях для подготовки персонала и повышения его квалификации, которые влияют на компетенцию отвечающих за документы специалистов, а также

l) отказ от проведения тестирования и актуализации плана действий в случае катастроф и в ходе последующего восстановления деятельности организации, что может повлиять на судьбу документов в случае стихийного бедствия.

5.3.2 Области неопределенности: технологические изменения

Внедрение новых технологий и систем создает возможности для совершенствования деловой деятельности, но при этом является областью неопределенности, где потенциально возможны негативные последствия. К числу областей неопределенности относятся:

a) технологические изменения, которые влияют на совместимость (интероперабельность) создающих или контролирующих документы систем;

b) совместимость с существующими платформами и системами;

c) планирование и осуществление миграции документов;

d) перераспределение ответственности и контроля над документными процессами;

e) эффективность внедрения изменений;

Пример - Адекватность планирования и управления проектом по внедрению новой платформы или программного обеспечения.

f) степень, в которой существующие политики охватывают внедренные организацией новые технологии;

Пример - Использование облачных сервисов, социальных сетей, RFID-радиометок, систем глобального позиционирования GPS/ГЛОНАСС.

g) способность внедряющих новые технологии системных администраторов и разработчиков осознавать влияние этих технологий на требования к документам - как на стадии проектирования, так и на этапе практической реализации;

Пример - Использование для разработки новых систем приложений для поддержки коллективной работы или вики-сред, не способных адекватным образом захватывать проектные документы и системную документацию.

h) способность существующей технической инфраструктуры удовлетворять новые требования, появившиеся в результате технологического развития организации или ее документных систем.

5.3.3 Области неопределенности: ресурсы - люди и компетенции

Выполнение организацией всех ее операций, включая документные процессы и эксплуатацию документных систем, зависит от наличия компетентного персонала. Специалисты по управлению документами или ответственные за документы лица проводят оценку областей неопределенности, включая следующие:

a) численность персонала, занятого созданием документов, контролем над ними, а также разработкой и поддержкой документных систем;

b) осведомленность о документных политиках и процессах;

c) поддержка высшим руководством деятельности по управлению документами;

d) осведомленность о связанных с документными процессами и системами рисках, и способность высшего руководства принимать решения по смягчению этих рисков;

e) управление взаимоотношениями между ответственными за документные системы лицами и пользователями;

f) адекватность компетенций персонала для создания документов и контроля над ними;

g) потеря ключевых специалистов, обладающих важнейшими навыками и глубокими знаниями организации и ее истории;

h) снижение со временем уровня квалификации персонала;

i) адекватность используемых средств оценки эффективности и пригодности персонала.

5.3.4 Области неопределенности: ресурсы - финансовые и материальные ресурсы

На финансовые и материальные ресурсы, доступные для адекватного управления документными процессами и системами, оказывают влияние как внешняя экономическая ситуация и деловая среда, так и уровень поддержки управления документами в организации. Области неопределенности включают в себя следующее:

a) достаточность финансовых ресурсов для исполнения обязательств и достижения целей управления документами;

b) достаточность финансовых ресурсов для закупки, обновления и поддержки адекватных систем.

5.4 Документные системы

При оценке воздействия риска на системы, используемые для создания документов и/или контроля над ними, следует принять во внимание архитектуру таких систем, вопросы обеспечения поддержки, жизнеспособности, непрерывности функционирования, интероперабельности и безопасности. Используемые организацией системы с течением времени сменяются в зависимости от экономических обстоятельств, перемен в характере деятельности и кадровом составе, а также в связи с изменениями размера и структуры организации. Критически важно, чтобы высшее руководство было надлежащим образом информировано о риске для документных систем и приняло на себя ответственность за предпринимаемые организацией меры реагирования.

Примечание 1 - В рамках настоящего подраздела термин "системы" следует понимать как "документные системы" в смысле определения, данного в 3.2.1.

Примечание 2 - Специалисты по управлению документами при проведении идентификации связанных с документными системами рисков в организациях, внедривших у себя меры и средства контроля и управления, предусмотренные стандартом системы менеджмента информационной безопасности ИСО/МЭК 27001, должны принять во внимание возможность

снижения рисков в некоторых областях благодаря этим мерам. В не внедривших ИСО/МЭК 27001 организациях, этот стандарт может быть использован как источник для выбора действий по смягчению риска из числа перечисленных в нем мер. Приложение С содержит таблицу, устанавливающую соответствие между относящимися к документным системам областями неопределенности и мерами контроля и управления, описанными в ИСО/МЭК 27001.

5.4.1 Области неопределенности: архитектура систем

Архитектура и конфигурация систем имеют ключевое значение для создания документов и обеспечения их долговечности. Данная область пересекается с идентификацией рисков для документных процессов. Адекватная документация по конфигурации системы является основой для решения вопросов, связанных как с другими областями риска на системном уровне, так и с процессами в системе.

Примечание - О документных процессах в системах см. 5.5.

Исходя из современного опыта, идентификация связанных с архитектурой систем рисков, особенно в контексте электронных документов, включает в себя следующее:

a) определение того, что является документом в системе, с тем чтобы система адекватно своим целям создавала документы и управляла ими;

Пример - В транзакционной базе данных следует выявить все необходимые элементы документа и обеспечить управление ими, с тем чтобы сведения о транзакции могли быть извлечены или воссозданы.

b) адекватное выявление требований в отношении сроков хранения;

Пример - В элементах (метаданных) документов должны быть указаны сами сроки хранения и события-"триггеры", запускающие отсчет сроков хранения и выполнение действий по уничтожению документов либо их передаче на архивное хранение.

c) выявление и документирование всех необходимых документных процессов, которыми должна управлять система;

d) эффективность архитектуры документных систем, соответствующая потребностям сотрудников организации и используемым организацией технологиям;

e) управление степенью зависимости от поддержки со стороны производителя системы;

f) доступ к документации производителя системы.

5.4.2 Области неопределенности: техническое обслуживание и поддержка

Техническое обслуживание документных систем в первую очередь относится к тем аспектам технологической платформы и поддержки систем, на которые влияют структурные изменения в организации, внедрение новых систем, изменения технологий, а также компетентность и надежность технической поддержки.

Области неопределенности включают в себя следующее:

a) изменения в деятельности и деловых системах, влияющие на документные системы;

b) уровень квалификации системных администраторов и понимание ими требований к

управлению документами в системах;

c) надежность поставщиков систем и их способность обеспечить техническое обслуживание систем и их постоянное соответствие текущему уровню развития технологий;

d) адекватность документации по процедурам оперативного технического обслуживания;

e) адекватность технической документации на системы;

f) адекватность документированных процедур резервного копирования и восстановления для документных систем;

g) адекватность процесса восстановления с резервных копий.

5.4.3 Области неопределенности: жизнестойкость и непрерывность функционирования

Жизнестойкость документных систем зависит от отслеживания перемен во внешнем и внутреннем контексте организации, с тем чтобы эти системы обновлялись, реагируя на изменяющиеся потребности.

При планировании действий по обеспечению непрерывного функционирования документных систем следует учитывать планы организации по обеспечению непрерывности деятельности. При отсутствии у организации плана по обеспечению непрерывности ее деятельности специалисты по управлению документами проводят анализ и оценку документных систем с целью установления приоритетов и процедур восстановления их работоспособности после перерывов в обслуживании.

Области неопределенности включают в себя следующее:

a) изменения во внешнем и внутреннем контексте, затрагивающие требования и потребности организации в отношении документов;

b) адекватность мониторинга качества документов и работы с ними, проводимого с целью выявления изменений в требованиях к документам;

c) адекватность оценки фактических затрат на внедрение и поддержание документных систем, включая затраты на оплату труда;

d) адекватность действий по выявлению и документированию документных систем;

e) поддержание и обеспечение доступности спецификаций и документации на документные системы;

f) адекватность документирования решений, принятых в ходе внедрения документных систем, и доступность этих документов всем нуждающимся в них пользователям;

g) способность документных систем поддерживать пригодность документов к использованию;

h) способность импортировать документы из унаследованных документных систем и прочих деловых систем;

i) проведение миграции документов в новую документную систему по причине изменения

требований к документам либо изменений в технологиях;

j) изменения в других системах, от которых зависит данная документная система;

k) способность облачных систем экспортировать документы, когда это необходимо, для их включения в собственные системы организации;

l) адекватность протоколирования истории событий в документной системе, включая обеспечение ее сохранности в течение срока службы системы; а также управление зависимостью от других систем с целью поддержания во времени осмысленности содержащейся в истории событий информации;

Пример - Ведение документации на уникальные идентификаторы, используемые в истории событий для обозначения пользователей и деловых подразделений.

m) способность документных систем поддерживать усилия по обеспечению непрерывности деятельности посредством предоставления доступа к необходимым документам в случае стихийного бедствия;

n) планирование действий на случай перебоев в обслуживании при возникновении нештатных ситуаций.

5.4.4 Области неопределенности: интероперабельность

Имеющиеся у документных систем зависимости и взаимосвязи с другими системами могут оказаться уязвимым местом.

Области неопределенности включают в себя следующее:

a) адекватность действий по выявлению и специфицированию необходимой интероперабельности между документными системами и иными деловыми системами;

b) зависимость документных систем от внешних по отношению к ним источников данных и способность обмениваться данными с этими системами, подключаться к ним либо ссылаться на их данные (примером могут служить облачные системы и другие внешние услуги по хранению данных);

c) совместимость стандартов и спецификаций, касающихся обмена документами и интероперабельности систем;

d) эффективность межсистемного взаимодействия (интероперабельности) после внесения изменений или проведения технологических обновлений одной или обеих взаимодействующих систем;

e) управление метаданными, относящимися к управлению документами, при перемещении документов между системами с тем, чтобы сохранить пригодность к использованию и смысл документов.

5.4.5 Области неопределенности: безопасность

Оценка риска, связанного с безопасностью документных систем, может проводиться с использованием серии стандартов ИСО/МЭК 27000 и использоваться в качестве элемента системы менеджмента информационной безопасности организации, если таковая имеется. Национальные стандарты и требования к информационной безопасности систем также могут

быть применимы в отношении документных систем.

Приложения B - D в ИСО/МЭК 27005 содержат примеры областей неопределенности, применимые в отношении любой информационной системы. Более специфические для документных систем области неопределенности также включают следующее:

a) адекватность политики безопасности организации в отношении документов, документных процессов и систем;

b) способность обеспечивать соблюдение и защиту правил и привилегий доступа, связанных с документами, документными процессами и системами;

c) политика и меры контроля в отношении действующих по поручению организации третьих сторон, влияющие на хранение, доступ и контроль над документами и документными системами.

5.5 Документные процессы

При идентификации риска основное внимание обращается на используемые при управлении документами и документными системами процессы создания документов (или их элементов) и контроля над ними.

Примечание - Предполагается, что специалисты по управлению документами при проектировании документов и документных процессов используют в качестве руководства стандарты и технические отчеты ИСО 15489-1, ИСО 23081-1, ИСО 23081-2 и ИСО/ТО 23081-3.

5.5.1 Области неопределенности: проектирование документов

Области неопределенности в процессах проектирования документов следующие:

a) адекватное проведение анализа видов деятельности с целью выявления требований к документам;

b) всесторонний характер сбора требований к документам для каждого делового процесса, когда, в том числе, учитываются потребности всех заинтересованных сторон;

c) адекватность проектирования документов (например, установления содержания и определения метаданных, необходимых для идентификации, описания, использования, сохранения истории событий, а также для планирования событий), соответствующая требованиям к документам;

d) адекватность схем наименования и классификации поставленным целям.

5.5.2 Области неопределенности: создание документов и внедрение документных систем

Области неопределенности в процессах создания документов и внедрения документных систем следующие:

a) для всех документов выбраны подходящие для соответствующих деловых процессов и документных систем точки их создания или захвата (обеспечиваются своевременность, комплексность и полнота создания/захвата);

b) эффективность интеграции, где это уместно, деловых процессов с процессами создания

документов и контроля над ними;

c) адекватное распределение и документирование обязанностей и ответственности создателей документов и участвующих в деловых транзакциях агентов (там, где это разные лица);

d) распределение обязанностей и ответственности по захвату документов организации из внешних сред соответствует требованиям;

e) спецификации метаданных ведутся и документируются надлежащим образом;

f) надлежащим образом документируются и контролируются процессы управления и протоколирования доступа к документам.

5.5.3 Области неопределенности: метаданные

Области неопределенности в процессах управления метаданными следующие:

a) имеются и доступны технические спецификации метаданных, используемых в документах, документных процессах и системах;

b) обеспечивается управление спецификациями метаданных, дающее возможность проводить по мере необходимости их обновление.

5.5.4 Области неопределенности: использование документов и документных систем

Области неопределенности в процессах доступа и использования следующие:

a) соответствующие требованиям стабильность и своевременность извлечения или получения доступа к документам;

b) адекватность управления правами доступа пользователей во всех документных процессах;

c) управление инцидентами безопасности и случаями взлома других мер и средств контроля доступа;

d) ведение документации, показывающей, кто во времени получал доступ к документам и вносил в них изменения;

e) адекватность подготовки использующего процессы персонала;

f) соблюдение установленных процедур.

5.5.4.1 Области неопределенности: поддержание пригодности к использованию

Области неопределенности в процессах поддержания пригодности к использованию следующие:

a) сохранение осмысленности метаданных документов во времени, особенно при наличии зависимости от данных из внешних систем или связей с ними;

b) адекватность документных процессов в плане сохранения аутентичности и надежности документов во времени;

c) поддержание доступности документов во времени;

d) управление применением шифрования документов в случае их передачи по каналам связи;

e) адекватность управления версиями документов во времени;

f) адекватность усилий по сохранению истории событий с документами с целью сохранения осмысленности документов во времени;

g) проблемы, связанные с устареванием оборудования и программного обеспечения (в том числе форматов), затрагивающие как документные процессы, так и документные системы.

Пример - Более старые версии электронных документов могут оказаться недоступными с использованием современных программных приложений (версий приложений).

5.5.5 Области неопределенности: уничтожение документов либо их передача на архивное хранение

Области неопределенности в процессах окончательного решения судьбы документов (их уничтожения либо передачи на архивное хранение) следующие:

a) уничтожение документов либо их передача на архивное хранение проводятся так, как это было запланировано и авторизовано;

b) процедуры окончательного решения судьбы документов предусматривают, в случае необходимости, возможность продолжения хранения документов после истечения срока их хранения;

Пример - Документы, необходимые в рамках судебного разбирательства либо запрошенные в соответствии с законодательством о свободе доступа к государственной информации, сроки хранения которых истекли.

c) документируются все действия, связанные с уничтожением либо передачей документов;

d) уничтожение документов надлежащим образом авторизовано и задокументировано;

e) проводится тестирование на предмет возможности восстановления информации с выведенного из эксплуатации оборудования и устройств хранения данных, в том числе с использованием методов и средств электронной судебно-криминалистической экспертизы.

Пример - Оценка адекватности использования переформатирования для уничтожения всех документов, хранящихся на жестких дисках компьютеров и копировально-множительных устройств или же на таких носителях информации, как флеш-накопители.

6 Анализ выявленных рисков

6.1 Общие положения

Риски анализируются путем определения их потенциальных последствий и возможности реализации.

В случае документных процессов и систем, последствия определяются в зависимости от области неопределенности и оцениваются в соответствии с критериями риска, установленными организацией согласно положениям раздела 4.

При этом следует принять во внимание существующие меры и средства контроля и управления, их действенность и эффективность.

6.2 Анализ возможности и количественная оценка вероятности реализации рисков

Под возможностью реализации риска (likelihood) понимается шанс (количественно оцениваемый через вероятность или частоту наступления событий) на то, что рисковое событие действительно произойдет. Анализ возможности реализации идентифицированных рисков проводится в соответствии с характером областей неопределенности и на основе данных за период времени, достаточно длительный для того, чтобы сделать заслуживающие доверия оценки.

Каждый риск следует оценивать как сочетание возможности того, что какое-то событие произойдет, и тех последствий, которые возникнут, если оно действительно случится.

Вероятности могут быть представлены по-разному, но обычно они взаимосвязаны с уровнем риска. При использовании качественных методов оценки на основе возможных последствий, вероятности и уровня риска устанавливается уровень значимости (такой, как "высокий", "средний" или "низкий").

В полуколичественных методах используются числовые рейтинговые шкалы для последствий и вероятности рисков, позволяющие на их основе определить уровень риска по формулам. Эти шкалы могут быть как линейными или логарифмическими, так и строиться на основе иных математических зависимостей; используемые формулы также могут различаться.

Чисто количественные методы, использующие количественные значения последствий и их вероятностей, могут быть использованы в тех случаях, когда имеются (статистические) данные о функционировании документных процессов и систем за достаточно длительный период времени.

В отношении документных процессов и систем может быть применим подход, при котором события классифицируются по частоте их реализации в течение времени, с присвоением каждой категории количественного показателя (баллов). Пример такой балльной оценки вероятности приведен в таблице 1.

Таблица 1

Пример балльной оценки вероятности

Оценка вероятности в баллах	Пояснения
1	Очень низкая вероятность, событие происходит не чаще, чем раз в 10 лет
2	Низкая вероятность, событие происходит не чаще, чем раз в 3 года

3	Средняя вероятность, событие происходит раз в год
4	Высокая вероятность, событие происходит чаще, чем раз в месяц

6.2.1 Контекст: внешние факторы

Оценка возможности наступления рисковых событий - в рамках социально-политической, макроэкономической и деловой сред, а также физической окружающей среды - опирается на историческую и текущую информацию, относящуюся к следующим категориям:

a) смена правительств и администраций;

b) статистическая и иная отчетность, отражающая макроэкономические показатели и данные о деятельности;

c) модели и тенденции социально-политических изменений в национальной и/или международной среде, имеющие существенное влияние в том месте, где располагается организация;

d) темпы изменений в технологиях и взаимосвязанных с ними темпов восприятия этих технологий обществом;

e) экстремальные погодные условия и иные неблагоприятные физические явления, включая, в том числе, перебои с функционированием инфраструктуры.

Исторические сведения об экстремальных погодных явлениях (например, ураганах) или о неблагоприятных физических событиях (таких, как пожары и масштабные отключения электричества) могут быть скудными или вообще отсутствовать, но из этого не следует, что эти события не могут произойти. Учитывая катастрофические последствия таких событий, при оценке рисков необходимо принимать во внимание подобную возможность.

6.2.2 Контекст: внутренние факторы

Оценка возможности наступления рисковых событий, связанных с изменениями в структуре и деятельности организации и в том, как она использует технологии и ресурсы, основываются на информации о недавней истории организации в следующих областях:

a) изменения в высшем руководстве (в том числе связанные с приватизацией, слияниями и поглощениями) и последовавшие вслед за ними перемены;

b) характерная реакция организации на внешние изменения, такие, как изменения, связанные с нормативно-правовой базой, технологическим развитием и финансовым климатом;

c) компетенция персонала и внутренняя система обучения и подготовки кадров;

d) текучесть кадров.

Такую историю недавних изменений следует рассматривать в контексте характера деятельности организации, ее размера и корпоративной культуры.

Пример - Организации с сильным акцентом на деловую конкуренцию или исторически склонные к лидерству в освоении новых технологий, с большей вероятностью внедрят новые технологии, чем некоммерческие организации по

оказанию услуг, чьими клиентами являются пожилые люди или социально незащищенные слои населения. Более вероятным фактором, способным заставить некоммерческие организации пойти на внутренние перемены, могут быть изменения в их финансировании. Оценка вероятных темпов внутренних преобразований основывается на информации, которая отражает специфику организации.

6.2.3 Системы

Оценка возможности наступления рисковых событий, связанных с системами, опирается на собранную информацию о безопасности, обеспечении непрерывности функционирования, о ресурсном обеспечения, интероперабельности и технической поддержке (в каждом случае идентифицируются аномалии, ошибки исполнения, нерешенные вопросы и проблемы, сведения о которых будут в дальнейшем использоваться для расчета или оценки частоты событий).

Вопросы безопасности документных систем, их интероперабельности и общие вопросы ресурсного обеспечения рассматриваются и документируются на стадиях их проектирования и анализа функционирования, в то время как планирование обеспечения непрерывности функционирования является одним из аспектов общей программы менеджмента деловых рисков организации.

Используемые при проектировании систем процессы могут оказаться уязвимыми для рисковых событий, способных повлиять на документные процессы в системе. Это следует учитывать при оценке возможности рисковых событий на этапе проектирования системы.

Анализ документов, созданных в рамках процедур технического обслуживания и поддержки, должен обеспечить прочную основу для оценки возможности неблагоприятных событий. Техническая поддержка системы охватывает вопросы как технологий, так и процедур.

Информацию, полученную в ходе проводимого в рамках контроля качества мониторинга с целью выявления несоответствий в процедурах технического обслуживания, следует проанализировать для того, чтобы оценить частоту появления несоответствий и выявить возможные повторяющиеся сценарии (patterns). Такие повторяющиеся сценарии несоответствий нужно анализировать в сопоставлении с проектными спецификациями системы.

Журналы (протоколы) аудита и аналогичные документы, отражающие нарушения системы безопасности и ограничения на доступ, следует аналогичным образом анализировать для выявления появляющихся сценариев и оценивания частоты и причин нарушений. Документы, подтверждающие проведение резервного копирования компьютеризованных систем в соответствии с проектными спецификациями, должны дать информацию, указывающую на возможные уязвимости и частоту их проявления.

При оценке возможности связанных с системами неблагоприятных событий следует учитывать приоритеты, установленные для различных документных систем.

6.2.4 Процессы

Процессы в сложившихся документных системах постепенно изменяются в результате прагматичного реагирования на аномалии или непредвиденные малозначительные события. Эти изменения, в отсутствие сознательного анализа и проведения документированных корректировок, со временем могут накопиться. Накопление небольших изменений в документных процессах представляет собой столь же значительную область неопределенности, как масштабные неблагоприятные внешние события. Возможность отклонения от проектных спецификаций оценивается на основе анализа несоответствий и авторизованных в особых обстоятельствах аномальных изменений.

Оценка возможности связанных с документными процессами рисковых событий основывается на информации, собранной при использовании документов, мер и средств контроля и управления над документами, а также таких инструментов, как классификационные схемы и указания по срокам хранения и действиям, выполняемых по их истечении.

Соответствующие источники информации включают в себя:

a) статистические данные о создании и использовании документов;

b) документы о несоответствиях по данным мониторинга, проводимого в рамках контроля качества;

c) документы об изменениях в схеме метаданных;

d) документы, отражающие использование указаний по срокам хранения и действиям, выполняемым по их истечении;

e) документы, отражающие изменения и нарушения ограничений на доступ.

На основе собранной информации может быть проведен анализ недочетов (gap analysis) для выявления тех направлений деятельности организации, в которых процессы создания документов не отвечают установленным требованиям либо сами требования изменились, а также новых направлений деятельности.

Анализ недочетов и документов о несоответствиях должны послужить основой для выявления проявляющихся повторяющихся сценариев изменений, на которые документные системы не смогли адекватно отреагировать, что указывает на наличие уязвимостей.

7 Сравнительная оценка рисков

7.1 Общие положения

Цель сравнительной оценки риска (risk evaluation), при которой устанавливается, является ли риск и/или его величина приемлемыми или допустимыми, заключается в том, чтобы помочь в принятии опирающихся на результаты анализа риска решений относительно того, на какие риски необходимо воздействовать, и о приоритете соответствующих действий.

Сравнительная оценка риска включает в себя сопоставление определенного в ходе процесса анализа уровня риска с критериями риска, установленными при изучении контекста деятельности организации. По итогам этого сравнения решается вопрос о необходимости воздействия на риск.

Масштабы последствий неблагоприятных событий и адекватность существующих мер и средств контроля и управления могут быть объединены с таблицей вероятностей, чтобы помочь с идентификацией рисков, которые должны быть в центре внимания мер, действий и воздействия на риск.

Могут быть приняты следующие решения:

a) требуется ли воздействие на риск;

b) приоритеты для воздействия на риски;

c) нужно ли выполнить какие-либо действия;

d) какой из возможных вариантов следует выбрать.

При сравнительной оценке риска на основе определения возможности и негативных последствий рисковых событий следует уделить должное внимание возможному воздействию редких и не имеющих прецедента происшествий, если их потенциальное воздействие расценивается как широкомасштабное и близкое к катастрофическому. Аналогичным образом воздействие накопившихся малозначительных нарушений или несоответствий может намного превысить воздействие каждого из них, если в совокупности они приведут к утрате целостности и надежности документов и документных систем.

Как отмечалось во введении, последствием рисковых событий для документных процессов и систем является утрата или повреждение документов, которые в результате становятся непригодными для использования, утрачивают надежность, аутентичность, полноту и/или неизменность, и могут поэтому не удовлетворять потребностям организации.

Рисковое событие может повлечь за собой целый ряд воздействий различного масштаба и воздействовать на достижение ряда различных целей и на различные заинтересованные стороны. Типы подлежащих анализу последствий и затронутые заинтересованные стороны идентифицируются тогда, когда организация устанавливает свои критерии для проекта по оценке рисков. При оценке воздействия связанных с документами изменений, неопределенности и неблагоприятных событий учитывается приданный документам приоритет. Приоритет документов отражается на оценке последствий в том, что неблагоприятное событие, в результате которого количество потерь было невелико, на деле может оказаться очень серьезным по своим последствиям, если были повреждены или утрачены документы, критически важные для реагирования на чрезвычайные ситуации либо отнесенные к числу ключевых деловых документов.

7.2 Оценка воздействия неблагоприятных событий

Необходимо принять во внимание следующие факторы:

a) число затронутых пользователей и других заинтересованных лиц;

b) последствия повреждения или утраты документов для оперативной деятельности организации;

c) уже реализованные меры реагирования на случай перебоев в доступе к документам;

d) время и усилия, требующиеся на восстановление или замену пострадавших документов;

e) последствия утраты или повреждения документов, подтверждающих права или собственность организации;

f) последствия утраты или повреждения документов, отражающих способность организации выполнить свои обязательства перед всеми заинтересованными сторонами;

g) нормативно-правовые требования по раскрытию информации об повреждении, утрате или несанкционированном доступе к документам;

h) последствия для репутации организации в обществе.

Данный перечень не является исчерпывающим. Выбор принимаемых во внимание факторов определяется в зависимости от размера и характера деятельности организации.

Потенциальное воздействие неблагоприятных событий может классифицироваться по образцу таблицы 2, с использованием факторов, признанных в наибольшей степени соответствующими размеру и характеру деятельности конкретной организации.

Таблица 2

Пример классификации воздействия неблагоприятных событий

Незначительные последствия	Умеренные последствия	Серьезные последствия	Тяжелые последствия
Аномальное нарушение ограничений доступа	Несанкционированный доступ к документам	Несанкционированный доступ к документам, факт которого следует раскрыть	Масштабная утрата, повреждение и/или несанкционированный доступ к документам
Повреждение небольшого числа документов, относящихся к одному направлению деятельности	Повреждение значительного числа документов, относящихся к одному направлению деятельности	Повреждение ключевых оперативных документов нескольких направлений деятельности	Повреждение ключевых документов большинства направлений деятельности
Ограниченная утрата данных	Утрата данных/потеря надежности	Утрата данных/потеря надежности; ущерб для репутации	Утрата данных/потеря надежности/потеря общественного доверия
Восстановимый ущерб	Оперативная деятельность не прерывается; восстановление документов требует усилий	Утрата официально признана; перебои в работе нескольких направлений деятельности; затратные меры по восстановлению деятельности	Остановка оперативной деятельности; затратные и отнимающие много времени меры по ее восстановлению; документы восстановить невозможно

7.3 Сравнительная оценка риска

Классификацию воздействия неблагоприятных событий можно объединить с таблицей вероятностей. Это поможет выявить неблагоприятные события, которые должны быть в центре внимания принимаемых в рамках менеджмента риска мер, начиная от процедур мониторинга и до планирования усилий по обеспечению готовности к чрезвычайным ситуациям.

Таблица 3 является примером того, как классификация воздействия неблагоприятных событий может быть соединена с оценками вероятностей и представлена в табличной форме.

Таблица 3

Пример сравнительной оценки риска

Событие			Вероятность	Последствия			
Контекст	Система	Процесс		Незначительные	Умеренные	Серьезные	Тяжелые
		Документы неправильно классифицированы, установлен неверный статус доступа	Высокая 1 раз в месяц или чаще	Исправляются в рамках существующих процедур			
Внесение изменений в законодательстве о защите персональных данных			Средняя 1 раз в год		Влияет на ограничения по доступу к кадровой системе; распространяется на другие операции		
	Сбой в работе функции индексирования в документной системе		Средняя 1 раз в год	Исправляются в рамках существующих процедур			

		Документы ошибочно отобраны на уничтожение	Средняя 1 раз в год	Исправляются в рамках существующих процедур			
		Неавторизованный доступ к документам, содержащим персональные данные сотрудников	Низкая 1 раз в 3 года		Неисправимые; сотрудникам приносятся извинения		
	Отсутствие электроэнергии в течение 8 часов		Низкая 1 раз в 3 года			Влияет на все документные системы; транзакции одного дня могут быть потеряны	
Пожаром уничтожено здание, в котором располагались документные системы			Очень низкая 1 раз в 10 лет				Утрата важных документов; перебои в оперативной деятельности; потеря общественного доверия

Сравнительная оценка риска документных процессов и систем организации должна выполняться в порядке приоритетов.

При применении таблицы 3 для указанной цели идентифицированное рисковое событие отражается (в соответствующей его категории графе) в левой части таблицы. В той же строке в правой части таблицы указываются уровень частоты и оценка воздействия данного события. Организация может дать балльную оценку воздействию и вероятности, и в итоге получить количественный показатель, отражающий приоритетность реагирования на данное рисковое событие.

8 Распространение информации о выявленных рисках

Оцененные риски должны быть задокументированы в реестре рисков (пример записи в реестре рисков см. в приложении А). Реестр рисков является инструментом для доведения информации о рисках до руководства организации. О зарегистрированных в реестре рисках и предлагаемых мерах реагирования на них должно быть поставлено в известность подразделение (служба) организации, ответственное за общую программу менеджмента риска в организации.

Основная цель анализа и распространения информации о рисках заключается в выявлении и установлении приоритетов и принятии надлежащих мер. Информирование о рисках является элементом эффективного менеджмента риска, обеспечивающим осведомленность о рисках и их признание в масштабе всей организации. Для того, чтобы обеспечить сохранение эффективности мер, выбранных для воздействия на риски, должен вестись мониторинг деятельности по оценке риска, а также регулярно проводиться ее анализ и совершенствование.

Приложение А
(справочное)

ПРИМЕР ЗАПИСИ О ДОКУМЕНТИРОВАННОМ РИСКЕ В РЕЕСТРЕ РИСКОВ

Таблица А.1

Описание риска	
Поля реестра	Сведения о риске
Идентификатор риска	4
Название риска	Неспособность установить лицо, создавшее документ
Тип и/или групповая принадлежность риска	Документы
Владелец риска	Системный администратор электронной системы управления документами и контентом (EDRMS)

Дата первичной идентификации риска	12 октября 2013 г.
Дата последнего обновления	15 октября 2013 г.
Описание	Невозможность установить, кто являлся автором зарегистрированного документа
Проявление риска (обстоятельства, при которых риск может материализоваться)	Неопределенность с тем, в деятельности какого именно из деловых подразделений образовался документ
Финансовый и иной ущерб в случае материализации риска	Низкий
Вероятность	Средняя
Последствия	Серьезные
Стратегия предотвращения риска	Провести анализ и доработку шаблонов документов в EDRMS-системе
Стратегия воздействия на риск	Провести анализ и доработку шаблонов документов в EDRMS-системе
Плановая дата	31 декабря 2013 г.
Ответственный за принятие мер	Системный администратор электронной системы управления документами и контентом (EDRMS)
Дата планового пересмотра	31 января 2014 г.
Ссылки на взаимосвязанные риски	3; 12
Статус риска и мер воздействия на него	Начаты действия по смягчению риска
Дата проведения последней оценки риска	15 октября 2013 г.

Приложение В
(справочное)

КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ВЫЯВЛЕНИЯ ОБЛАСТЕЙ НЕОПРЕДЕЛЕННОСТИ

Примечание - Данное приложение представляет собой пример списка контрольных вопросов (контрольного списка), который организация может использовать на регулярной основе для выявления изменений и областей неопределенности, появившихся в течение установленного периода времени (например, ежегодно).

В.1 Внешние факторы

B.1.1 Общественно-политический контекст

Внедрен ли в организации процесс мониторинга изменений во внешних условиях ее деятельности?

Фиксируются ли в ходе проводимого организацией мониторинга изменения в следующих областях:

a) изменения в законодательно-нормативной базе, влияющие на требования к документам?

b) изменения в государственной политике, затрагивающие требования к документам, документные процессы и системы?

c) новые кодексы практики или изменения в стандартах, касающихся документных процессов и систем?

d) изменения потребностей в связанных с документами услугах?

e) изменения ожиданий заинтересованных сторон в отношении документов?

Имели ли место в прошедшем году какие-либо события или изменения внешних обстоятельств, которые повлияли на репутацию организации или общественный статус?

B.1.2 Макроэкономическая и технологическая среда

Имели ли место в прошедшем году какие-либо изменения в форме собственности, структуре или функциях организации?

Имели ли место изменения в выручке, клиентской базе, иные изменения деловой среды, которые повлияли на требования к документам?

Были ли изменения в нормативном регулировании или в частоте и характере судебных споров?

Имело ли место технологическое развитие общества в целом, потенциально способное повлиять на организацию?

B.1.3 Физическая среда и инфраструктура

Учтены ли при планировании действий по обеспечению готовности к чрезвычайным ситуациям региональные и местные экстремальные погодные явления и другие стихийные бедствия?

Учтены ли при планировании действий по обеспечению готовности к чрезвычайным ситуациям техногенные катастрофические события (акты войны или терроризма, крупные аварии)?

Готова ли организация на случай перебоев с оказанием услуг, способных повлиять на документные системы и на хранения документов?

B.1.4 Внешние угрозы безопасности

Являются ли адекватными меры информационной безопасности, используемые для защиты документных систем от несанкционированного доступа и/или намеренного причинения

вреда?

Является ли адекватной система физической безопасности мест и систем хранения документов организации (как в бумажном, так и в электронном виде) и проводятся ли регулярные проверки ее состояния?

Ведется ли надлежащий мониторинг и регулярная проверка безопасности ИТ-систем организации?

Есть ли у организации планы на случай возможных перебоев с получением необходимых для документных систем услуг и сервисов третьих сторон?

B.2 Внутренние факторы

B.2.1 Организационные изменения

Установлена ли во всех подразделениях организации задокументированная ответственность за документы (например, назначены их владельцы)?

Внедрены ли процедуры для управления передачей и миграцией документов, а также объединением систем вслед за изменениями в структуре организации?

В случаях передачи документов или смены их владельца, были ли затем права доступа согласованы соответствующими сторонами и задокументированы?

Есть ли возможность легко объединить документные системы с другими системами в случае, если произойдут крупные изменения в структуре организации и характере ее деятельности?

Имеется ли адекватная документация на документные системы (включая унаследованные), и является ли она доступной?

Включены ли надлежащие договорные условия относительно права собственности на документы, контроля над ними и отслеживания сроков их хранения в контракты и соглашения об использовании аутсорсинга, облачных услуг и перевода в оффшоры (оффшоринга)?

Как отразится на организации изменение условий в контрактах на оказание третьими сторонами услуг по поддержке/управлению документными системами?

Внедрен ли процесс регулярного пересмотра и обновления политик и процедур, относящихся к документным системам?

Были ли при планировании предусмотрены резервы на случай решения проблем, связанных с потерей ключевых сотрудников, отвечавших за документные системы и процессы?

Внедрены ли для документных систем процедуры реагирования на связанные с персоналом изменения (т.е. на обучение, изменение оплаты труда и сокращение численности)?

Имеется ли процедура пересмотра и обновления планов обеспечения готовности к действиям в нештатных ситуациях вслед за проведением организационных изменений?

B.2.2 Технологические изменения

Могут ли технологические изменения повлиять на функциональную совместимость

(интероперабельность) документных систем с другими системами?

Совместимы ли меняющиеся технологии с используемыми в данный момент платформами документных систем и операционными системами?

Является ли процедура проведения миграции документов/систем актуальной, документированной и адекватной?

Имеются ли процессы, обеспечивающие полноту миграции метаданных документов при внедрении новых технологий, и проводится ли проверка на предмет порчи или утраты информации при миграции?

Внедрены ли процессы, предотвращающие как несанкционированное уничтожение, так и избыточно длительное хранение переставших быть нужными документов в случаях, когда проводится миграция или обновление систем?

Внедрена ли процедура для управления изменениями конфигурации документных систем и процессов?

Является ли актуальным и задокументированным распределение ответственности за изменения конфигурации документных систем, процессов и мер и средств контроля и управления?

Обеспечивается ли надлежащее управление проектом внедрения изменений в технологии, влияющие на документные системы?

Адекватно ли текущие политики отражают новые технологии по мере их внедрения организацией?

Осознают ли ИТ-специалисты и руководители, когда внедряют новые технологии, какие последствия те повлекут для документных систем и системной документации?

Способна ли существующая технологическая инфраструктура организации обеспечить поддержку технологических изменений в документных системах?

В.2.3 Ресурсы: люди и компетенции

Является ли текущая численность персонала достаточной для выполнения документных процессов и управления документными системами?

Адекватно ли информирован персонал организации о политиках и процессах, связанных с документами?

Поддерживает ли высшее руководство деятельность по управлению документами?

Рассматривает ли высшее руководство риски для документных процессов и систем как риски для всей организации, которые необходимо снижать или устранять?

Включаются ли в должностные инструкции, где это уместно, обязанности и ответственность за работу с документами?

Влияет ли текущая или достижимая способность реагировать на изменения во внешней нормативно-правовой среде на политику и процедуры организации по управлению документами?

Являются ли обязанности системных администраторов документных систем по отношению к пользователям этих систем четко определенными и задокументированными?

Обеспечивают ли существующие процессы передачу важнейших знаний, навыков и умений вести оперативную деятельность среди ответственного за документы персонала?

Доступна ли для ответственного за документы персонала программа непрерывного обучения?

Ведется ли мониторинг уровня знаний, навыков и компетенций ответственного за документы персонала?

B.2.4 Ресурсы: финансовые и материальные ресурсы

Адекватно ли финансируется управление документами для достижения целей соответствующей политики и для выполнения в организации процедур управления документами?

Обеспечиваются ли адекватное финансирование и поддержка документных систем, в том числе их обновление и техническое обслуживание?

B.3 Документные системы

B.3.1 Архитектура систем

Включает ли системная документация определение того, что представляют собой все элементы документов?

Имеется ли адекватная документация на метаданные и процессы в системе?

Обеспечено ли адекватное управление в документной системе и документирование всех требований в отношении сроков хранения?

Все ли документные процессы, которыми управляет система, идентифицированы и документированы?

Соответствует ли выбранная технология размеру, сложности и характеру деятельности организации?

Обеспечивает ли технология адекватную поддержку функциональных возможностей документной системы?

Зависит ли система от поддержки поставщика, является ли договор об оказании услуг действующим, и достаточно ли четко определены эти услуги?

Является ли адекватной документация поставщика, охватывает ли она все необходимые элементы и схемы кодирования?

B.3.2 Техническое обслуживание и поддержка

Часто ли происходят изменения в конструкции систем и иных их аспектах, таких как безопасность?

Существуют ли в организации адекватные процедуры управления изменениями,

обеспечивающие авторизованность, плановость и контролируемость изменений в системах?

Являются ли уровень квалификации системных администраторов и их понимание требований к документам в системах надлежащими и актуальными?

Проводится ли регулярный анализ способности поставщиков систем поддерживать их в актуальном состоянии?

Является ли документация на процедуры технического обслуживания и поддержки документных систем доступной, регулярно пересматриваемой и обновляемой?

Осуществляется ли мониторинг и документирование отказов и ненормального функционирования технологий, влияющих на работу документных систем?

Является ли документация на технические системы доступной и актуальной?

Проводится ли регулярное тестирование и пересмотр процессов резервного копирования и восстановления для документных систем? Являются ли эти процессы документированными?

В.3.3 Жизнестойкость и непрерывность функционирования

Проводится ли регулярный мониторинг и анализ функционирования документных систем в увязке с изменениями во внешнем и внутреннем контексте, влияющими на требования организации к документам?

Анализируются ли данные мониторинга качества функционирования документных систем с целью обновления требований к документам или внесения в них иных изменений?

Проводилась ли оценка финансовых ресурсов, требующихся для адекватного внедрения и поддержания документных систем, и для привлечения соответственно компетентного персонала к управлению этими системами?

Выявила ли организация все системы, которые создают документы, хранят их и управляют ими?

Документируются ли надлежащим образом спецификации документных систем, и являются ли они доступными?

Установлены ли и задокументированы ли процедуры оперативного технического обслуживания?

Документируются ли решения, принимаемые в ходе внедрения документных систем, обеспечивается ли их сохранность и доступность всем тем пользователям, которым они нужны?

Проводится ли регулярное тестирование способности документных систем поддерживать пригодность документов к использованию?

Ведется ли регулярный мониторинг и подготовка отчетности об эксплуатационных показателях документных систем, в сопоставлении с поставленными перед ними целями?

Существует ли установленная процедура управления миграцией документов в новую документную систему?

Имеется ли у документных систем проверенная возможность импорта документов из

унаследованных систем или из иных деловых систем?

Ведется ли мониторинг и управление изменениями в других системах, от которых данная документная система зависит либо с которыми она связана иным образом?

В случае использования услуг внешних поставщиков, таких как услуги облачного хранения, проводилось ли тестирование возможности экспорта документов и их обратного включения в собственные документные системы организации?

Проводится ли регулярный анализ истории событий в документных системах, и обеспечивается ли надлежащее управление их зависимостями от других систем?

Охватывает ли планирование обеспечения непрерывности деятельности конкретно документные системы?

Способствуют ли документные системы обеспечению непрерывности деятельности путем предоставления доступа к документам в случае чрезвычайных ситуаций?

Имеются ли планы действий в чрезвычайных ситуациях, предусматривающие управление случаями перебоев в работе сервисов, обслуживающих документные системы?

B.3.4 Интероперабельность

Выявила ли организация требования к интероперабельности (функциональной совместимости) между деловыми системами и системами, в которых хранятся документы; были ли подготовлены соответствующие спецификации?

Обеспечено ли выявление, документирование и надлежащее управление зависимостями документных систем от внешних источников данных или от иных систем, включая внешние услуги и сервисы, такие как услуги облачного хранения?

Использует ли организация, в целях выполнения выявленных требований к интероперабельности, совместимые стандарты или спецификации, чтобы обеспечить устойчивый обмен документами между соответствующими системами?

Организован ли мониторинг и надлежащее управление изменениями (такими как обновления программного обеспечения) в системах, от которых документные системы зависят или с которыми им необходимо взаимодействовать?

Адекватно ли документируется обмен документами между системами в метаданных обеих систем, управляется ли он надлежащим образом?

B.3.5 Безопасность

Соответствие мер и средств обеспечения информационной безопасности, описанных в ИСО/МЭК 27001, и положений настоящего стандарта, установлено в приложении С.

Примечание - Приложения B - D в ИСО/МЭК 27005 также содержат примеры областей неопределенности, применимые в отношении любой информационной системы.

Адекватно ли в политике безопасности (информационной безопасности) организации отражены вопросы безопасности документов, документных процессов и систем?

Обеспечивается ли на практике соблюдение и документирование ограничений прав

пользователей на доступ, создание и модификацию документов?

Внедрены ли процедуры безопасности, обеспечивающие изменение прав доступа пользователей к системам в случаях, когда изменяются выполняемые сотрудниками роли или когда с ними прекращаются трудовые отношения?

Существуют ли политика и процедуры контроля над выполняемой по поручению организации деятельностью третьих сторон, которая связана с защищенным хранением, доступом и обработкой документов и с документными системами?

Проводится ли регулярная оценка действенности политики и мер информационной безопасности; выполняются ли корректирующие действия?

B.4 Документные процессы

B.4.1 Проектирование документов

Является ли анализ требований к документам и потребностей деятельности организации в документах:

a) основанным на адекватном знании деятельности организации,

b) всесторонним и комплексным,

c) учитывающим все соответствующие нормативно-правовые требования, а также

d) учитывающим интересы всех заинтересованных сторон?

Охватывает ли процесс проектирования все задокументированные варианты использования существующих документов о деятельности организации?

Обеспечивает ли процесс проектирования документов выполнение в каждой конкретной системы требований к метаданным, связанных с идентификацией, описанием, использованием документов, протоколированием истории событий и планированием событий?

Соответствуют ли правила именования и классификационные схемы (там, где они применяются) используемой организацией терминологии?

B.4.2 Создание документов и внедрение документных систем

Адекватен ли процесс создания или захвата документов соответствующим деловому процессу и системе, т.е. является ли он надежным, систематическим, своевременным, опирающимся на подходящую технологию?

Обеспечивается ли надлежащая идентификация документов и контроль над ними, начиная от момента их захвата или создания?

Является ли процесс создания или захвата документов интегрированным, насколько это возможно, с деловым процессом либо тесно связанным с завершением транзакции?

Получили ли создатели документов надлежащую подготовку по процессам?

Задокументированы ли должным образом обязанности и ответственность за создание и захват документов, и проводится ли, где это уместно, различие между ними и обязанностями

пользователей деловой системы?

Установлены, распределены и задокументированы ли обязанности и процессы для захвата документов из внешних сред?

Соответствует ли доступ к документам нормативно-правовым требованиям; обеспечены ли его надлежащее протоколирование и мониторинг?

В.4.3 Метаданные

Являются ли спецификации метаданных (включая их технические спецификации) документированными, существует ли возможность их обновлять?

В.4.4 Использование документов и документных систем

Есть ли у пользователей возможность стабильного доступа к документам, тогда, когда они в них нуждаются?

Управляются ли надлежавшим образом права доступа пользователей системы на создание/захват, получение доступа и модификацию документов?

Устанавливаются ли права доступа на основе выполняемых ролей, а не индивидуально?

Сохраняется ли документированная информация о доступе к содержащимся в системе документам и их модификации?

Есть ли в системе возможности для преодоления ограничений доступа, являются ли они документированными и внедрены ли надлежащие механизмы для разрешения такого рода конфликтов?

Имеют ли пользователи документов надлежащую подготовку по использованию процессов документных систем?

Внедрены ли процессы для предотвращения неправильного использования или несанкционированного раскрытия документов?

В.4.5 Поддержание пригодности к использованию

Адекватно ли документируется и остается ли доступным во времени контекст создания и использования документов?

Внедрены ли механизмы для управления зависимостями (такими, как ссылки на данные и т.п.) документов от внешних систем, поддерживающие возможность понимать и правильно интерпретировать документы?

Являются ли надежными, документированными и постоянно контролируемыми процессы, обеспечивающие надежность и аутентичность документов во времени (например, меры по предотвращению несанкционированного доступа или модификации)?

В случае использования шифрования при хранении/передаче документов, обеспечивается ли возможность их расшифровки?

Обеспечивается ли доступность истории версий документа, а также относящихся к нему поправок, комментариев и заметок до тех пор, пока в этом сохраняется необходимость?

Ведутся ли истории связанных с документами событий адекватным образом, так чтобы обеспечить сохранение с течением времени возможности понимать их?

Внедрена ли процедура контроля пригодности к использованию более старых документов, с учетом, например их зависимости от оборудования и программного обеспечения, адекватности используемых способов физического хранения для документов различного формата?

B.4.6 Уничтожение документов либо их передача на архивное хранение

Имеются ли актуальные и адекватные указания по срокам хранения документов и действиям по их истечении?

Существует ли процесс пересмотра существующих указаний по срокам хранения?

Имеются ли процедуры для окончательного решения судьбы документов по истечении сроков их хранения - уничтожения, передачи на архивное хранение и т.д.?

Установлены и задокументированы ли роли и обязанности по проведению уничтожения документов либо их передачи на архивное хранение?

Проводится ли уничтожение/передача на архивное хранение документов регулярно, в рамках нормальной деятельности?

a) Имеется ли процесс для разрешения исключительных ситуаций?

b) Ведется ли надлежащее документирование процессов уничтожения/передачи на архивное хранение, в том числе принятых решений?

c) Проводится ли соответствующее обучение ответственных за документы сотрудников по вопросам проведения уничтожения/передачи на архивное хранение?

d) Используются ли методы уничтожения, адекватные требованиям по безопасности?

Внедрены ли процессы, обеспечивающие полноту и необратимость уничтожения документов, с учетом необходимости предотвратить восстановление документов с электронных устройств и носителей информации?

Приложение C
(справочное)

РУКОВОДСТВО ПО ИСПОЛЬЗОВАНИЮ МЕР И СРЕДСТВ ИЗ ПРИЛОЖЕНИЯ A "ЦЕЛИ И МЕРЫ УПРАВЛЕНИЯ" ИСО/МЭК 27001

При идентификации связанных с системами рисков в организациях, которые внедрили предусмотренные ИСО/МЭК 27001 меры и средства контроля и управления, специалисты по управлению документами должны принимать во внимание то, как некоторые из этих мер действуют на смягчение рисков в ряде областей неопределенности. В организациях, внедривших меры из ИСО/МЭК 27001, выполнению специалистами по управлению документами оценки риска для документных процессов и систем будет способствовать глубокое понимание стандарта и согласование с ним. В организациях, где ИСО/МЭК 27001 не внедрялся,

предлагаемые им меры могут быть использованы в качестве источника при выборе действий по смягчению риска. В этой связи настоятельно рекомендуется дальнейшее ознакомление со стандартами системы менеджмента информационной безопасности серии ИСО/МЭК 27001.

Приведенная ниже таблица устанавливает соответствие между перечисленными в 5.4 настоящего стандарта областями неопределенности и мерами, предусмотренными ИСО/МЭК 27001.

Где это уместно, в правой графе таблицы "Комментарии" приводятся замечания и советы, помогающие взглянуть на меры по обеспечению информационной безопасности из ИСО/МЭК 27001 с точки зрения документных систем.

Таблица С.1

N п/п	Настоящий стандарт, 5.4. Области неопределенности для документных систем	ИСО/МЭК 27001:2013, приложение А. Цели и меры управления	Комментарии
Области неопределенности: архитектура систем			
1	Определение того, что является документом в системе, с тем чтобы система адекватно своим целям создавала документы и управляла ими	Соответствующих мер нет	
2	Адекватное выявление требований в отношении сроков хранения	Соответствующих мер нет	Уничтожение документов по истечении срока их хранения не относится к центральным вопросам информационной безопасности, однако с точки зрения документных систем это важная область неопределенности, особенно в том случае, если создающие и контролирующие документы системы не обеспечивают исполнение на практике решений, принятых в отношении сроков хранения и действий по их истечении

3	Выявление и документирование всех необходимых документных процессов, которыми должна управлять система	Соответствующих мер нет	
4	Эффективность архитектуры документных систем, соответствующая потребностям сотрудников организации и используемым организацией технологиям	**A.10.3.1 Управление производительностью** Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности	Требования к производительности и использование ресурсов - это единственные два аспекта оценки эффективности документных систем, которые должны быть в первую очередь протестированы на соответствие требованиям оперативной деятельности
5	Управление степенью зависимости от поддержки со стороны производителя системы	**A.12.5.5 Разработка программного обеспечения с привлечением сторонних организаций** Разработка программного обеспечения с привлечением сторонних организаций должна производиться под контролем и при мониторинге организации	Если документные системы базируются на коммерческом программном обеспечении, поставляемом внешним поставщиком, то надежность этого поставщика необходимо принять во внимание при идентификации рисков. Предлагаемая ИСО/МЭК 27001 мера может носить слишком общий характер с точки зрения документных систем
6	Доступ к документации производителя системы	**A.10.1.1 Документирование операционных процедур эксплуатации** Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей	В случае документных систем предусмотренную ИСО/МЭК 27001 меру следует применять в отношении любой программной документации, которая описывает внутренние процедуры по поддержке этих документных систем
Области неопределенности: техническое обслуживание и поддержка			
1	Изменения в деятельности и деловых системах, влияющие на	**A.10.1.2 Управление изменениями** Изменения в конфигурациях средств обработки информации и системах	Предусмотренные ИСО/МЭК 27001 меры следует дополнить требованиями о распространении информации,

	документные системы	должны быть контролируемыми **А.10.10.4 Журналы регистрации действий администратора и оператора** Действия системного администратора и системного оператора должны быть регистрируемыми **А.10.10.5 Регистрация неисправностей** Неисправности должны быть зарегистрированы, проанализированы и устранены	обеспечивающими ознакомление специалистов по управлению документами с такого рода изменениями
2	Уровень квалификации системных администраторов и понимание ими требований к управлению документами в системах	**А.10.3.1 Управление производительностью** Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности **А.10.3.2 Приемка систем** Должны быть определены критерии принятия новых и модернизованных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки	Предусмотренные ИСО/МЭК 27001 меры нельзя считать достаточными для смягчения рисков, связанных с компетентностью системных администраторов в части требований к документам. Этому вопросу необходимо уделить особое внимание
3	Надежность поставщиков систем и их способность обеспечить техническое обслуживание систем и их постоянное соответствие текущему уровню развития технологий	**А.12.5.5 Разработка программного обеспечения с привлечением сторонних организаций** Разработка программного обеспечения с привлечением сторонних организаций должна производиться под контролем и при мониторинге организации	Если документные системы базируются на коммерческом программном обеспечении, поставляемом внешним поставщиком, то надежность этого поставщика необходимо принять во внимание при идентификации рисков. Предлагаемая ИСО/МЭК 27001 мера может носить слишком общий характер с точки зрения документных систем
4	Адекватность документации по процедурам	**А.10.1.1 Документирование операционных процедур эксплуатации**	Системная документация (техническая документация и описания процедур) должна

	оперативного технического обслуживания	Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей	рассматриваться в качестве официальных документов и поддерживаться соответствующим образом
5	Адекватность технической документации на системы	**A.10.1.1 Документирование операционных процедур эксплуатации** Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей	Системная документация (техническая документация и описания процедур) должна рассматриваться в качестве официальных документов и поддерживаться соответствующим образом
6	Адекватность документированных процедур резервного копирования и восстановления для документных систем	**A.10.5.1 Резервирование информации** Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования	Предусмотренная ИСО/МЭК 27001 мера в отношении резервного копирования/восстановления не охватывает весь спектр неопределенностей, связанных с поддержанием пригодности к использованию и уничтожением документов
7	Адекватность процесса восстановления с резервных копий	**A.10.5.1 Резервирование информации** Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования	Предусмотренная ИСО/МЭК 27001 мера в отношении резервного копирования/восстановления не охватывает весь спектр неопределенностей, связанных с поддержанием пригодности к использованию и уничтожением документов
Области неопределенности: жизнестойкость и непрерывность функционирования			
1	Изменения во внешнем и внутреннем контексте, затрагивающие требования и потребности организации в отношении документов	Соответствующих мер нет	

2	Адекватность мониторинга качества документов и работы с ними, проводимого с целью выявления изменений в требованиях к документам	**A.10.10.1 Ведение журналов аудита** Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа **A.10.10.2 Мониторинг использования средств обработки информации** Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации	Предусмотренные ИСО/МЭК 27001 меры отражают один из аспектов мониторинга работы системы, однако в документных системах необходимо проводить более обширный мониторинг с целью обеспечения качества их функционирования
3	Адекватность оценки фактических затрат на внедрение и поддержание документных систем, включая затраты на оплату труда	**A.6.1.3 Распределение обязанностей по обеспечению информационной безопасности** Обязанности персонала по обеспечению информационной безопасности должны быть четко определены **A.10.3.1 Управление производительностью** Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности	Предусмотренные ИСО/МЭК 27001 меры не охватывают экономические аспекты использования систем, за исключением меры, устанавливающей ответственность за информационную безопасность внутри организации Экономические аспекты документных систем могут оказаться важной областью неопределенности в организациях, проводящих политику сокращения расходов
4	Адекватность действий по выявлению и документированию документных систем	**A.7.1.2 Владение активами** Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение представителя организации. Примечание - Термин	Предусмотренная ИСО/МЭК 27001 мера обращает внимание на необходимость документировать владельцев систем, однако адекватное выявление и документирование документных систем тоже

		"владелец" (owner) определен как лицо или организация, на которую возложена установленная ответственность управления по контролю производства, разработке, поддержке, использованию и безопасности активов. Термин "владелец" не означает, что данное лицо или организация фактически имеет права собственности на этот актив	нужны
5	Поддержание и обеспечение доступности спецификаций и документации на документные системы	**А.10.7.4 Безопасность системной документации** Системная документация должна быть защищена от несанкционированного доступа	Предусмотренная ИСО/МЭК 27001 мера ориентирована на защиту документации с целью избежать рисков информационной безопасности. С точки зрения документных систем, при этом возникает неопределенность с тем, будет ли документация доступна в случае необходимости. Защиту и доступность следует балансировать, поскольку обе они являются источниками потенциальных рисков
6	Адекватность документирования решений, принятых в ходе внедрения документных систем, и доступность этих документов всем нуждающимся в них пользователям	**А.10.7.4 Безопасность системной документации** Системная документация должна быть защищена от несанкционированного доступа	См. выше
7	Способность документных систем поддерживать пригодность документов к использованию	Соответствующих мер нет	Пригодность к использованию не находится в центре внимания информационной безопасности, однако с точки зрения управления документами здесь может быть существенная область неопределенности

8	Способность импортировать документы из унаследованных документных систем и прочих деловых систем	Соответствующих мер нет	
9	Проведение миграции документов в новую документную систему по причине изменения требований к документам либо изменений в технологиях	**A.12.5.2 Технический анализ прикладных систем после внесения изменений в операционные системы** При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации	Помимо изменений в операционных системах, миграцию от одной системы к другой следует выделить как область неопределенности, связанную с поддержанием во времени свойств документов
10	Изменения в других системах, от которых зависит данная документная система	Соответствующих мер нет	
11	Способность облачных систем экспортировать документы, когда это необходимо, для их включения в собственные системы организации	Соответствующих мер нет	
12	Адекватность протоколирования истории событий в документной системе, включая обеспечение ее сохранности в течение срока службы системы; а также управление зависимостью от	**A.10.10.1 Ведение журналов аудита** Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля	Предусмотренный в ИСО/МЭК 27001 журнал аудита действий пользователей является, с точки зрения управления документами, ограниченным по содержанию. В журнале аудита должны также отражаться другие действия с документами, чтобы сформировать адекватную историю событий

	других систем, с целью поддержания во времени осмысленности содержащейся в истории событий информации	доступа	
13	Способность документных систем поддерживать усилия по обеспечению непрерывности деятельности посредством предоставления доступа к необходимым документам в случае стихийного бедствия	**A.14.1.3 Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность** Должны быть разработаны и внедрены планы для поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критических бизнес-процессов **A.14.1.4 Структура плана обеспечения непрерывности бизнеса** Должна быть создана единая структура планов непрерывности бизнеса, позволяющая обеспечить непротиворечивость всех планов для последовательного выполнения всех требований к информационной безопасности и для расстановки приоритетов при тестировании и обслуживании **A.14.1.5 Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса** Планы по обеспечению непрерывности бизнеса должны подлежать регулярному пересмотру и обновлению с целью обеспечить их актуальность и эффективность **A.15.1.3 Защита учетных**	Предусмотренные ИСО/МЭК 27001 меры по менеджменту непрерывности деятельности сфокусированы на требованиях по информационной безопасности. С точки зрения управления документами, эти меры могут быть дополнены требованиями к документам, в центре внимания которых находятся важнейшие для оперативной деятельности документы

		записей организации Важные учетные записи организации должны быть защищены от утраты, разрушения и фальсификации в соответствии с требованиями, установленными законами, документами органов исполнительной власти, контрактами и требованиями бизнеса	
14	Планирование действий на случай перебоев в обслуживании при возникновении нештатных ситуаций	**A.14.1.3 Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность** Должны быть разработаны и внедрены планы для поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критических бизнес-процессов	Предусмотренные ИСО/МЭК 27001 меры по менеджменту непрерывности деятельности сфокусированы на требованиях по информационной безопасности. С точки зрения управления документами, эти меры могут быть дополнены требованиями к документам, направленными на решение проблем обеспечения непрерывности деятельности
Области неопределенности: интероперабельность			
1	Адекватность действий по выявлению и специфицированию необходимой интероперабельности между документными системами и иными деловыми системами	**A.10.8.1 Политики и процедуры обмена информацией** Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов **A.10.8.2 Соглашения по обмену информацией** Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением **A.10.8.5 Системы бизнес-информации**	Предусмотренные ИСО/МЭК 27001 меры делают упор на формальное документирование процедур обмена информации между системами в интересах информационной безопасности. С точки зрения управления документами, интероперабельность между документными и иными системами имеет значение для нормальной повседневной оперативной деятельности, и следовательно это более широкая область неопределенности. Перебои во взаимодействии систем могут повлиять на доступность документов и их пригодность к использованию

		Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации	
2	Зависимость документных систем от внешних по отношению к ним источников данных и способность обмениваться данными с этими системами, подключаться к ним либо ссылаться на их данные (примером могут служить облачные системы и другие внешние услуги по хранению данных)	**A.6.2.1 Определение рисков, связанных со сторонними организациями** Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности **A.6.2.3 Рассмотрение требований безопасности в соглашениях со сторонними организациями** Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации	С точки зрения управления документами, безопасность данных, находящихся в распоряжении поставляющих услуги третьих сторон - не единственный фактор, который следует учесть, однако предлагаемые меры являются, тем не менее, адекватными
3	Совместимость стандартов и спецификаций, касающихся обмена документами и интероперабельности систем	**A.15.2.2 Проверка технического соответствия требованиям безопасности** Информационные системы следует регулярно проверять на соответствие требованиям стандартов безопасности	Предусмотренные ИСО/МЭК 27001 меры сфокусированы на стандартах обеспечения безопасности. С точки зрения управления документами, поскольку использование этого стандарта в отношении документных систем также может стать областью неопределенности, охват мер

			следует расширить на стандарты обмена документами и интероперабельности
4	Эффективность межсистемного взаимодействия (интероперабельности) после внесения изменений или проведения технологических обновлений одной или обеих взаимодействующих систем	**A.10.3.2 Приемка систем** Должны быть определены критерии принятия новых и модернизованных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки	
5	Управление метаданными, относящимися к управлению документами, при перемещении документов между системами с тем, чтобы сохранить пригодность к использованию и смысл документов	Соответствующих мер нет	Способность документных систем поддержать выполнение требований к метаданным может быть важной областью неопределенности. Если документные системы не в состоянии обеспечить надлежащее управление метаданными из документных процессов, то могут пострадать смысл и значение документов и их пригодность к использованию
Области неопределенности: безопасность (Вся данная область должна покрываться мерами и средствами контроля и управления из ИСО/МЭК 27001. Приведенные ниже примеры отражают наиболее существенные меры.)			
1	Адекватность политики безопасности организации в отношении документов, документных процессов и систем	**A.5.1.1 Документирование политики информационной безопасности** Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций **A.5.1.2 Анализ политики информационной безопасности**	При идентификации рисков в данной области специалисты по управлению документами должны обеспечить, чтобы политика организации в сфере информационной безопасности учитывала конкретные потребности, связанные с документами и документными системами. Они также должны обеспечить согласованность политики и процедур управления

		Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности	документами с политикой информационной безопасности
2	Способность обеспечивать соблюдение и защиту правил и привилегий доступа, связанных с документами, документными процессами и системами	**A.11.1.1 Политика контроля доступа** Политика контроля доступа должна быть установлена и документирована с учетом потребностей бизнеса и безопасности информации **A.11.2.1 Регистрация пользователей** Должна быть установлена формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам **A.11.2.2 Управление привилегиями** Предоставление и использование привилегий должно быть ограниченным и контролируемым **A.11.2.3 Управление паролями пользователей** Предоставление паролей должно быть контролируемым посредством формализованного процесса управления **A.11.2.4 Пересмотр прав доступа пользователей** Руководство должно периодически осуществлять пересмотр прав доступа пользователей, используя формализованный процесс **A.11.6.1 Ограничения доступа к информации** Доступ к информации и функциям прикладных систем пользователей и	При идентификации рисков в данной области специалисты по управлению документами должны учитывать ограничения на права пользователей в отношении доступа, создания и модификации документов. Права доступа должны быть приведены в соответствие с установленной политикой управления доступом, являющейся частью политики информационной безопасности

		обслуживающего персонала должен быть предоставлен только в соответствии с определенными политиками контроля доступа	
3	Политика и меры контроля в отношении действующих по поручению организации третьих сторон, влияющие на хранение, доступ и контроль над документами и документными системами	**A.6.2.3. Рассмотрение требований безопасности в соглашениях со сторонними организациями** Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации **A.10.2.1 Оказание услуг** Должна быть обеспечена уверенность в том, что меры управления информационной безопасностью, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией **A.10.2.2 Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями** Необходимо регулярно проводить мониторинг, аудит и анализ услуг, отчетов и актов, обеспечиваемых сторонней организацией **A.10.2.3 Изменения при оказании сторонними организациями услуг по обеспечению безопасности** Изменения при оказании услуг по обеспечению безопасности, включая	

		внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков	

Приложение ДА
(справочное)

СВЕДЕНИЯ О СООТВЕТСТВИИ ССЫЛОЧНЫХ МЕЖДУНАРОДНЫХ СТАНДАРТОВ НАЦИОНАЛЬНЫМ СТАНДАРТАМ РОССИЙСКОЙ ФЕДЕРАЦИИ

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO Guide 73:2009	IDT	ГОСТ Р 51897-2011/Руководство ИСО 73:2009 "Менеджмент риска. Термины и определения"
ISO 15489-1:2001	IDT	ГОСТ Р ИСО 15489-1-2007 "Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования"
ISO 23081-1:2006	IDT	ГОСТ Р ИСО 23081-1-2008 "Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы"
ISO 23081-2:2009	-	<*>
ISO/TR 23081-3:2011	-	<*>
ISO/IEC 27001:2013	-	<*>
ISO/IEC 27005:2011	-	<*>
ISO 30300:2011	IDT	ГОСТ Р ИСО 30300-2015 "Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Системы управления

		документами. Основные положения и словарь"
ISO 31000:2009	IDT	ГОСТ Р ИСО 31000-2010 "Менеджмент риска. Принципы и руководство"
IEC 31010:2009	IDT	ГОСТ Р ИСО/МЭК 31010-2011 "Менеджмент риска. Методы оценки риска"
<*> Соответствующий национальный стандарт отсутствует. Примечание - В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: - IDT - идентичные стандарты.		

Библиография

[1] ISO 15489-1:2001, Information and documentation - Records management - Part 1: General

[2] ISO/TR 15489-2:2001, Information and documentation - Records management - Part 2: Guidelines

[3] ISO 23081-1:2006, Information and documentation - Records management processes - Metadata for records - Part 1: Principles

[4] ISO 23081-2:2009, Information and documentation - Managing metadata for records - Part 2: Conceptual and implementation issues

[5] ISO/TR 23081-3:2011, Information and documentation - Managing metadata for records - Part 3: Self-assessment method

[6] ISO 27001, Information technology - Security techniques - Information security management systems - Requirements

[7] ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

[8] ISO 31000:2009, Risk management - Principles and guidelines

[9] IEC 31010:2009, Risk management - Risk assessment techniques