ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54471— 2011/ISO/TR 15801:2009

Системы электронного документооборота

УПРАВЛЕНИЕ ДОКУМЕНТАЦИЕЙ. ИНФОРМАЦИЯ, СОХРАНЯЕМАЯ В ЭЛЕКТРОННОМ ВИДЕ

Рекомендации по обеспечению достоверности и надежности

ISO/TR 15801:2009
Document management — Information stored electronically — Recommendations for trustworthiness and reliability
(IDT)

Издание официальное

Москва
Стандартинформ
2012

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», а правила применения национальных стандартов Российской Федерации — ГОСТ Р 1.0—2004 «Стандартизация в Российской Федерации. Основные положения»

Сведения о стандарте

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «Электронные Офисные Системы (проектирование и внедрение)» на основе собственного аутентичного перевода на русский язык стандарта, 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 18 октября 2011 г. № 466-ст

4 Настоящий стандарт идентичен техническому отчету ИСО/ТО 15801—2009 «Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности» (ISO/TR 15801—2009 «Document management — Information stored electronically — Recommendations for trustworthiness and reliability»).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5 (пункт 3.5).

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

Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячно издаваемых информационных указателях «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном указателе «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

© Стандартинформ, 2012

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

Содержание

1 Область применения . . . 1
2 Термины и определения . . . 1
3 Политика управления информацией . . . 1
3.1 Общие положения . . . 1
3.2 Документ, определяющий политику управления информацией . . . 2
4 Надлежащая предусмотрительность (duty of care) . . . 4
4.1 Общие положения . . . 4
4.2 Менеджмент информационной безопасности . . . 5
4.3 Планирование мер по обеспечению непрерывности деловой деятельности (business continuity planning) . . . 6
4.4 Консультации с заинтересованными сторонами (consultations) . . . 6
5 Процессы и процедуры . . . 7
5.1 Общие положения . . . 7
5.2 Руководство по процедурам (procedures manual) . . . 7
5.3 Сбор и включение в систему (capture) информации . . . 8
5.4 Создание и включение в систему (capture) графических образов документов . . . 10
5.5 Сбор и включение в систему (capture) данных . . . 14
5.6 Индексирование . . . 15
5.7 Процедуры создания заверенных копий электронной информации (authenticated output procedures) . . . 16
5.8 Передача файлов . . . 17
5.9 Сохранение бумажных документов (document retention) . . . 18
5.10 Обеспечение долговременной сохранности информации . . . 19
5.11 Уничтожение информации . . . 19
5.12 Резервное копирование и восстановление системы . . . 19
5.13 Техническая поддержка (maintenance) системы . . . 20
5.14 Безопасность и защита . . . 20
5.15 Использование услуг, оказываемых по контракту . . . 21
5.16 Автоматизация деловых операций (workflow) . . . 23
5.17 Отметки даты и времени . . . 23
5.18 Контроль версий . . . 23
5.19 Поддержание документации в актуальном состоянии (maintenance of documentation) . . . 24
6 Ключевые технологические вопросы (enabling technologies) . . . 25
6.1 Общие положения . . . 25
6.2 Руководство по системе (system description manual) . . . 25
6.3 Выбор носителей информации и подсистемы хранения (storage media and sub-system considerations) . . . 25
6.4 Уровни доступа . . . 26
6.5 Контроль целостности системы (system integrity checks) . . . 26
6.6 Обработка графических образов . . . 27
6.7 Методы сжатия . . . 28
6.8 Разделение формы и введенной информации, «снятие» формы (form overlays and form removal) . . . 29
6.9 Факторы окружающей среды (environmental considerations) . . . 29
6.10 Миграция . . . 29
6.11 Удаление и/или уничтожение (expungement) информации . . . 29
7 Контроль информации (audit trails) . . . 30
7.1 Общие положения . . . 30
7.2 Контрольная информация по системе . . . 32
7.3 Контрольная информация, относящаяся к сохраняемой информации . . . 33
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации . . . 35
Библиография . . . 36

Введение

Настоящий стандарт содержит описание рекомендуемой практики электронного хранения деловой и иной информации в электронной форме. Выполнение приведенных рекомендаций полезно для организации даже когда достоверность хранимой информации не оспаривается.

Информация в виде цифровых объектов берет свое начало из многих источников. Настоящий стандарт применим к электронным объектам в любой форме, от традиционных отсканированных графических образов, электронных таблиц и подготовленных в текстовых редакторах документов и до более «современных» форм, таких как электронная почта, веб-контент, мгновенные сообщения, файлы чертежей, подготовленных в системах автоматизированного проектирования, блоги, вики и т. д.

Пользователи настоящего стандарта должны понимать, что реализация данных рекомендаций не обеспечивает автоматической приемлемости электронной информации в качестве доказательств. В тех случаях, когда электронная информация может потребоваться в суде, применяющим настоящий стандарт лицам и организациям рекомендуется обратиться за юридической консультацией, чтобы уточнить, какие именно законодательные и нормативные требования на них распространяются.

В стандарте описаны меры и средства, с помощью которых в любое время можно продемонстрировать, что контент конкретного электронного объекта, созданного или существующего в компьютерной системе, не изменился с момента его создания в этой системе или с момента импорта в нее.

Независимо от того, каким был оригинальный формат информации, можно будет доказать, что сохраненная в надежной системе информация надежно и устойчиво воспроизводится и что она точно, без каких-либо существенных изменений, отражает то, что было первоначально сохранено.

В тех случаях, когда на законных основаниях возможна подготовка других версий информации (например, новой редакции договора), новые версии рассматриваются как новые электронные объекты. Такой же подход может применяться и тогда, когда в среде автоматизации деловых процессов (workflow-среде) в документ вносятся существенные изменения.

Системы управления информацией могут хранить в электронном виде как информацию, так и документы (в соответствии с определением, приведенным в ГОСТ Р ИСО 15489-1). Настоящий стандарт описывает меры и средства, позволяющие сохранять все виды электронной информации надежным и заслуживающим доверия образом. В случае хранения документов требования настоящего стандарта могут использоваться совместно с требованиями ГОСТ Р ИСО 15489-1 с тем, чтобы обеспечить согласованность использования описанных в стандарте политик и процедур с предусмотренными в стандарте ГОСТ Р ИСО 15489-1.

Пользователям следует применять настоящий стандарт совместно с законами, нормативными правовыми актами и иными документами, устанавливающими обязательные для исполнения требования на федеральном, региональном, муниципальном и отраслевом уровнях.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системы электронного документооборота

УПРАВЛЕНИЕ ДОКУМЕНТАЦИЕЙ. ИНФОРМАЦИЯ, СОХРАНЯЕМАЯ В ЭЛЕКТРОННОМ ВИДЕ

Рекомендации по обеспечению достоверности и надежности

Electronic records management systems. Document management. Information stored electronically. Recommendations for trustworthiness and reliability

Дата введения — 2012—08—01

1 Область применения

Настоящий стандарт описывает порядок внедрения и эксплуатации систем управления информацией и документами, которые могут рассматриваться как надежно, заслуживающим доверия образом, хранящие электронную информацию.

Настоящий стандарт может применяться в любой организации, которая использует систему управления информацией для сохранения во времени аутентичной, надежной и пригодной к использованию/читаемой электронной информации. Такие системы включают в себя политики, процедуры, технологии и требования к аудиту, обеспечивающие поддержание целостности электронной информации при хранении.

Настоящий стандарт не охватывает процессы, используемые для оценки аутентичности информации до ее сохранения либо импорта в систему. Настоящий стандарт, однако, может использоваться для доказательства того, что с момента сохранения информации в системе выдаваемая системой информация будет верным и точным воспроизведением оригинала.

В рамках настоящего стандарта термин «система», если явно не указано иное, означает оцениваемую систему управления информацией.

2 Термины и определения

В настоящем стандарте применены термины по ИСО 12651, а также следующие термины с соответствующими определениями:

2.1 **тип информации** (information type): Группы взаимосвязанных информационных материалов.

Примечание — В конкретных приложениях «группы» могут обозначаться терминами «наборы», «дела», «коллекции» и т. п.

Пример — Инвойсы, финансовые документы, сводки, переписка.

2.2 **доверенная система** (trusted system): Система <управления информацией>, используемая для сохранения электронной информации и обеспечивающая ее точность, надежность, пригодность к использованию/читаемость, а также целостность во времени.

3 Политика управления информацией

3.1 Общие положения

Информация является одним из наиболее важных активов, имеющихся в распоряжении любой организации. Все виды деятельности организации включают в себя то или иное использование информации. Количество информации может быть огромным, и существует множество различных способов ее

Издание официальное

представления и хранения. Ценность используемой информации и то, каким образом она применяется и перемещается как внутри, так и между организациями, может стать решающим фактором успеха или провала этих организаций.

Информацию, подобно любым другим активам, необходимо классифицировать, структурировать, проверять, оценивать, защищать, контролировать, измерять и ею нужно эффективно и продуктивно управлять.

Настоящий подраздел содержит описание документации, в которой сформулирована политика организации в области управления информацией. Кроме того, настоящий подраздел содержит рекомендации для организаций относительно уровня документирования, необходимого для того, чтобы они смогли ясно и четко регламентировать, каким образом обеспечиваются надежность, точность и достоверность информации, содержащейся в доверенных системах управления информацией. Наличие такой документации также может служить доказательством того, что управление информацией и документами является частью нормальных процедур деловой деятельности.

Если в системе хранится информация, которая может быть использована в качестве доказательств в ходе каких-либо судебных разбирательств или деловых процессов, то организации необходимо проконсультироваться с юристами (см. 4.4), чтобы обеспечить исполнение соответствующих законодательно-нормативных требований. Поскольку законодательно-нормативные требования в различных странах, регионах и отраслях могут различаться, то правовой анализ должен охватывать все юрисдикции, в которых действует организация, и все сферы ее деятельности.

3.2 Документ, определяющий политику управления информацией

3.2.1 Содержание

Должен быть разработан внутренний нормативный документ (далее – «политика»), документирующий политику организации в области управления и хранения информации применительно к доверенным системам управления информацией.

Политика должна содержать разделы, в которых:

- указывается, какая информация подпадает под действие данной политики (см. 3.2.2);
- сформулирована политика в отношении носителей информации (см. 3.2.3);
- сформулирована политика в отношении файловых форматов электронных объектов и контроля версий (см. 3.2.4);
- сформулирована политика в отношении соответствующих стандартов управления информацией (см. 3.2.5);
- определены политики в области сохранения в течение установленных сроков хранения и уничтожения информации (см. 3.2.6);
- определена ответственность за управление информацией (см. 3.2.7);
- определены обязанности за контроль исполнения этой политики (см. 3.2.8).

Политика должна быть утверждена высшим руководством организации и регулярно пересматриваться.

С точки зрения настоящего стандарта ключевым элементом является утверждение и применение на практике перечня видов документов и информации, образующихся в деятельности организации, с указанием сроков хранения и действий по их истечении (далее — «перечень»). Везде, где в остальной части стандарта делается ссылка на политику, также подразумевается и перечень.

3.2.2 Информация, подпадающая под действие политики

Для того чтобы можно было сформулировать политику, информацию следует сгруппировать по типам так, чтобы политика в отношении всей информации одного типа была согласованной. Например, тип информации может определяться путем указания на ее применение (например, финансовые прогнозы, счета, список адресов клиентов) или по связи с определенными бизнес-процессами (например, заявления, жалобы, просьбы о продлении оказания услуг), либо ссылкой на родовые группы (например, на данные бухгалтерского учета, документы о клиентах, производственную документацию).

В ходе подготовки проекта политики, возможно, определенную информацию потребуется перегруппировать с тем, чтобы обеспечить согласованность политики в отношении информации, относящейся к одному типу.

В политике следует перечислить все подлежащие хранению типы информации. В их числе следует упомянуть документы, разработанные во исполнение положений политики (например, внутренние нормативные документы по отдельным вопросам).

3.2.3 Носители информации

Разные типы носителей информации имеют различные характеристики в плане их долговременного хранения. Большинство организаций использует для хранения информации различные типы носите-

лей: бумагу, микроформы, электронные (как носители однократной записи, так и перезаписываемые/стираемые) или оптические (как носители однократной записи, так и перезаписываемые/стираемые) носители. В некоторых приложениях определенная информация может в течение своего срока хранения в разные периоды времени храниться на носителях различных типов.

Организации следует регламентировать использования конкретных типов носителей информации для удовлетворения различающихся требований к хранению информации (таких, например, как требования к доступности информации, сроки хранения и требования по безопасности). Соответствующие положения должны быть детализированы в политике.

Для каждого типа информации (см. 3.2.2) должны быть указаны типы носителей, на которых эту информацию следует сохранять.

При наличии копий (экземпляров) электронных объектов может быть важно иметь возможность доказать, что никакие изменения в них не вносились. Если электронные объекты существуют в различных версиях, то для целей настоящего стандарта каждая версия должна рассматриваться как новый первоисточник или оригинальный объект.

Положения, регламентирующие управление копиями электронных объектов, должны быть детализированы в политике.

3.2.4 Файловые форматы и сжатие данных

Политика должна содержать сведения о допустимых файловых форматах, которые могут быть использованы для каждого типа информации (см. 3.2.2).

Для извлечения и отображения любой сохраняемой в компьютерной системе информации требуется программное обеспечение. Это программное обеспечение подвержено изменениям либо из-за выпуска новых версий, либо вследствие изменений в операционных системах и/или аппаратном обеспечении. Благодаря реализации на практике политики использования утвержденных файловых форматов и (если таковые применяются) технологий сжатия данных могут быть успешно выполнены необходимая миграция данных или альтернативные процедуры, обеспечивающие долговременное использование хранимой информации.

В случае использования методов сжатия политика их применения должна быть задокументирована.

Если возможно сохранение нескольких версий информации или документов, то необходимо разработать порядок и правила, обеспечивающие сохранение всех подлежащих хранению версий, а также поддержание взаимосвязей между ними. Положения, регламентирующие хранения версий информации и документов, должны быть включены в политику.

Дополнительную информацию по этому вопросу см. 5.5.2, 5.10, 6.10 и 7.2.3.

3.2.5 Стандарты, относящиеся к управлению информацией

Если в организации действует система менеджмента качества (например, на основе стандартов ИСО серии 9000), полностью или частично охватывающая доверенную систему управления информацией, то вся соответствующая документация о процедурах должна быть включена в системы менеджмента качества.

При наличии обязательных национальных или международных требований или в тех случаях, когда применимы национальные или международные стандарты, следует исполнять соответствующие требования и положения стандартов.

3.2.6 Указания по срокам хранения и действиям по их истечении (retention and disposal schedules)

Сроки хранения и действия по их истечении должны быть установлены для каждого типа информации.

Сроки хранения должны быть согласованы со всеми соответствующими подразделениями и должностными лицами организации.

Сроки хранения должны устанавливаться после проведения соответствующих консультаций, обеспечивающих надлежащее решение правовых вопросов и исполнение законодательно-нормативных требований.

Для всей создаваемой соответствующей системной и процедурной документации должны быть установлены сроки хранения.

Указания по срокам хранения и действиям по их истечении должны включать в себя политику организации по их периодическому пересмотру.

Указания по срокам хранения и действиям по их истечении должны включать в себя политику организации в отношении контролируемого уничтожения информации.

3.2.7 Ответственность за управление информацией

Политика должна устанавливать индивидуальную и (или) должностную ответственность за ее разработку и актуализацию.

Следует идентифицировать и включить в политику индивидуальную и (или) должностную ответственность за каждый тип информации.

Индивидуальная и должностная ответственность должна предусматривать обязанность обращаться за соответствующими консультациями при разработке или актуализации политики.

3.2.8 Соответствие положениям политики

Если важно иметь возможность продемонстрировать соответствие положениям политики, то следует идентифицировать и включить в политику индивидуальную и (или) должностную ответственность за достижение и поддержание такого соответствия.

4 Надлежащая предусмотрительность (duty of care)

4.1 Общие положения

4.1.1 Доверенная система (trusted system)

Доверенной является такая система управления документами и информацией, которая позволяет рассматривать всю сохраняемую в ней в электронном виде информацию как достоверные и точные копии первоначальной информации независимо от ее первоначального формата. Доверенные системы управления документами и информацией должны, как минимум, обеспечивать:

- создание не менее одной копии сохраненной информации на носителе, защищающем эту информацию от модификации, внесения неавторизованных дополнений или удаления на протяжении установленного для нее жизненного цикла; такая копия должна сохраняться и поддерживаться в безопасном месте, расположенном отдельно от места хранения других копий хранимой информации;

- использование оборудования и носителей информации, защищающих хранимую информацию от модификации, внесения неавторизованных дополнений или удаления на протяжении установленного для нее жизненного цикла (см. также 6.3);

- возможность с помощью предусмотренных методологиями использования программного обеспечения, аппаратных средств и/или носителей информации процессов независимого аудита убедиться в том, что первоначально сохраненная информация может быть точно воспроизведена на всем протяжении установленного для нее жизненного цикла.

В доверенной системе управления документами и информацией используется в соответствии с указаниями настоящего стандарта сочетание организационной политики, оперативных процедур и надлежащим образом реализованных и поддерживаемых технологий, позволяющее использующей систему организации подтверждать достоверность и надежность сохраняемой в ней информации.

4.1.2 Меры контроля (controls)

Очень важно, чтобы организация осознавала значение проектирования и поддержания всех аспектов доверенной системы управления документами и информацией и выполняла свои обязанности в соответствии с принципом проявления должной предусмотрительности (duty of care).

Для этого выполнения этой задачи организация должна:

- установить порядок подотчетности (chain of accountability) и распределить на всех уровнях ответственность за действия, связанные с управлением электронной информацией;

- знать, какие законодательные и регулирующие органы имеют отношение к ее деятельности;

- быть в курсе технических, процедурных, нормативных и законодательных изменений, поддерживая контакты с соответствующими органами и организациями;

- внедрить политику обеспечения информационной безопасности.

4.1.3 Разделение обязанностей (segregation of roles)

Разделение обязанностей является одним из фундаментальных аспектов надлежащей предусмотрительности и обеспечивает возможность проверки на наличие ошибок и преднамеренной фальсификации документов (в этом отношении разделение обязанностей особенно важно в тех системах, в которых существует риск мошенничества или других злонамеренных действий).

Есть несколько аспектов управления документами и информацией, для которых рассматривается возможность применения разделения ответственности:

- контроль полноты вводимой информации и ее соответствия установленным требованиям (inputreconciliation) (см. 5.4.3);

- контроль качества (см. 5.4.6);

- ввод данных (см. 5.6);

- удаление информации (см. 5.11);
- обеспечение информационной безопасности (см. 4.2).

Кроме того, важно обеспечить, чтобы имеющие отношение к системе физические и организационно-административные разграничения зеркально отражались в используемых в системе мерах логического управления доступом.

Следует проанализировать возможность применения и по мере необходимости реализовать разделение обязанностей по выполнению первичных операций и контролю над ними.

4.2 Менеджмент информационной безопасности

4.2.1 Политика информационной безопасности

Вся информация независимо от вида носителей, на которых она хранится, уязвима и подвержена риску утраты или изменения, как случайного, так и злонамеренного. Для защиты информации, сохраняемой в электронном виде, необходимо разработать и внедрить меры безопасности, позволяющие снизить риск успешного оспаривания ее аутентичности. Эти меры безопасности должны соответствовать используемым грифам конфиденциальности/секретности.

Традиционно информационная безопасность рассматривается как вопрос конфиденциальности, с тем чтобы обеспечить доступ к информации строго в соответствии с установленными организацией требованиями. И хотя это действительно важно (а в ряде случаев критически важно) для функционирования организации, это не самая важная из проблем безопасности с точки зрения вопросов, рассматриваемых в настоящем стандарте.

Одной из главных целей политики информационной безопасности является обеспечение защиты целостности хранимой информации. При разработке мер безопасности необходимо сопоставить риск компрометации целостности с затратами на осуществление таких мер. Меры безопасности должны охватывать резервные и иные копии хранимой информации, поскольку их целостность важна в тех случаях, когда они используются взамен/для замены хранящихся в системе данных.

Также важна доступность информации. Иногда может возникнуть необходимость доказать, что вся информация по определенному вопросу в любое время доступна для анализа. Для этой цели ключевыми являются такие вопросы, как точность индексирования и планирование обеспечения непрерывности деловой деятельности.

Безопасность — не единственная проблема компьютерных систем. Ключевыми элементами являются как защищенность, так и доступность операционной среды (в том числе зданий, систем контроля температурного режима, сетевых соединений и т. д.), и проверяемое выполнение процедур всем персоналом.

Организации следует ввести политику информационной безопасности, охватывающую все элементы доверенной системы управления документами и информацией.

Если в организации уже имеется политика информационной безопасности для других систем, то вопросы использования доверенной системы управления документами и информацией следует включить в область применения этого документа.

Политика информационной безопасности должна, как минимум, содержать:

- область применения политики;
- цели управления в области обеспечения безопасности;
- конкретные положения политики;
- требования в отношении информации, имеющей различные грифы конфиденциальности/секретности;
- определение и распределение ответственности за обеспечение информационной безопасности;
- политику реагирования на нарушения (инциденты) безопасности;
- политику соблюдения соответствующих стандартов.

Политика информационной безопасности должна быть одобрена высшим руководством организации. Это одобрение должно быть задокументировано.

Организация должна согласовать и задокументировать надлежащие уровни безопасности, обеспечиваемые при управлении информацией и соответствующие политике информационной безопасности организации.

Следует рассмотреть вопрос о соответствии требованиям ГОСТ Р ИСО/МЭК 27001. Что касается доверенных систем управления документами и информацией, то при проработке необходимых мер контроля и управления, обеспечивающих исполнение требований ГОСТ Р ИСО/МЭК 27001, следует учитывать требования настоящего стандарта.

4.2.2 Оценка рисков (risk assessment)

Меры безопасности нередко разрабатываются на основе индивидуального (adhoc) подхода в качестве реакции на инциденты безопасности или исходя из имеющихся программных средств. При использовании таких процедур в системе безопасности часто остаются слабые места, которые закрываются лишь впоследствии. Более структурированный подход предусматривает анализ информационных активов организации и определение факторов риска (на основе ценности активов, уязвимости системы и вероятности атак). После этого может быть подготовлена и утверждена политика информационной безопасности, на соответствие которой может проводиться аудит мер безопасности.

Организации следует провести анализ рисков информационной безопасности и задокументировать полученные результаты.

Особое значение имеют меры безопасности, осуществляемые для контроля над носителями информации, используемыми как в действующей системе, так и для резервного копирования. Анализ рисков должен учитывать факторы риска наличия уязвимостей, соответствующие типу используемого носителя информации (например, это может быть WORM-носитель однократной записи либо перезаписываемый носитель).

Если применяются различные типы носителей информации, следует проанализировать их влияние на результаты анализа риска.

По завершении анализа риска по его итогам должны приниматься меры в рамках проводимой оценки эффективности уже реализованных мер безопасности. В ходе процесса анализа необходимо принимать во внимание такие факторы, как баланс между стоимостью реализации мер, достигнутым уровнем безопасности и оценкой риска.

На основе результатов анализа риска должна быть проведена оценка эффективности существующих мер безопасности.

Если результаты анализа указывают на то, что имеет смысл изменить процедуры обеспечения безопасности, то следует осуществить такие изменения.

4.2.3 Концепция информационной безопасности (information security framework)

Для запуска и дальнейшего контроля над внедрением в организации системы информационной безопасности следует разработать концепцию менеджмента. Целями этой концепции должны быть:

- утверждение и пересмотр политики информационной безопасности;
- мониторинг угроз информационной безопасности;
- мониторинг и анализ нарушений безопасности;
- одобрение главных инициатив по повышению информационной безопасности.

4.3 Планирование мер по обеспечению непрерывности деловой деятельности (business continuity planning)

Время от времени у доверенных систем управления документами и информацией могут возникать проблемы, для устранения последствий которых потребуется выполнение нештатных процедур (emergencyprocedures). Такие процедуры могут предусматривать временное использование дополнительных ресурсов или ресурсов сторонних организаций. В целях обеспечения того, чтобы в ходе подобных операций не компрометировалась целостность информации, может быть реализован согласованный и утвержденный план обеспечения непрерывности деловой деятельности (иногда его называют «планом восстановления после катастроф»).

Процедуры, которые предполагается использовать в случаях серьезных отказов оборудования, экологических и кадровых проблем, следует разрабатывать, проверять и поддерживать. Процедуры должны обеспечивать, чтобы в ходе их выполнения не компрометировалась целостность хранимой информации.

4.4 Консультации с заинтересованными сторонами (consultations)

Применение доверенных системы управления документами и информацией может иметь существенные последствия для других организаций и лиц, таких как:

- контролирующие органы;
- государственные органы;
- органы внешнего аудита;
- юридические консультанты (например, юристы организации).

До начала осуществления политики управления документами и информацией организации следует провести консультации с соответствующими организациями и лицами, заинтересованными в аутентичности, надежности и целостности хранимой информации.

В ходе консультаций могут быть затронуты:

- вопросы национального и международного права;

- вопросы регулирования конкретной отрасли;
- нормативные акты муниципальных властей;
- политика организации;
- процедуры в подразделениях;
- права отдельных лиц.

Организация должна провести консультации с соответствующими организациями до начала осуществления политики управления документами и информацией.

Эти консультации могут охватывать следующие темы:

- правовые вопросы;
- государственные законодательно-нормативные требования;
- требования к финансовой деятельности (например, по уплате налогов);
- специальные требования (применимые к конкретным отраслям).

Политика должна включать в себя или ссылаться на результаты консультаций, включая согласованные, запланированные или осуществленные действия.

Если существуют соответствующие нормативные требования и/или законы, их следует соблюдать.

В политике следует указывать, нужно ли полностью или частично исполнять требования соответствующих национальных и международных стандартов.

Если организация исполняет требования соответствующих национальных и международных стандартов, то этим требованиям должна соответствовать и доверенная система управления документами и информацией.

5 Процессы и процедуры

5.1 Общие положения

В настоящем разделе рассматриваются процедуры, связанные с функционированием доверенной системы управления документами и информацией.

5.2 Руководство по процедурам (procedures manual)

5.2.1 Документация

Для каждой доверенной системы управления документами и информацией организация должна вести руководство по процедурам (procedures manual).

Везде, где в настоящем разделе установлены требования к наличию какой-либо документации, руководство по процедурам может включать в себя эту документацию либо ссылаться на нее. Руководство по процедурам может содержать, там где это уместно, ссылки на иную контролируемую документацию.

Процедуры, которые описывает либо на которые ссылается руководство по процедурам, должны быть легкодоступны для всех авторизованных пользователей системы.

5.2.2 Содержание

Руководство по процедурам должно включать в себя или ссылаться на процедуры использования доверенной системы управления документами и информацией и охватывать следующие вопросы:

- сбор и включение в систему информации (см. 5.3);
- сбор и включение в систему графических образов документов (см. 5.4);
- сбор и включение в систему данных (см. 5.5);
- индексирование (см. 5.6);
- процедуры создания заверенных копий электронной информации (см. 5.7);
- передача файлов (см. 5.8);
- сохранение документов (см. 5.9);
- обеспечение долговременной сохранности информации (см. 5.10);
- уничтожение информации (см. 5.11);
- резервное копирование и восстановление системы (см. 5.12);
- поддержание системы (см. 5.13);
- безопасность и защита (см. 5.14);
- использование услуг, оказываемых по контракту (см. 5.15);
- автоматизация деловых операций (workflow) (см. 5.16);
- отметки даты и времени (см. 5.17);
- контроль версий (см. 5.18);
- ведение документации (см. 5.19).

Для удобства допускается ведение руководства по процедурам в виде нескольких отдельных физических документов, относящихся к различным областям управления документами и информацией.

Если в организации имеется несколько доверенных систем управления документами и информацией, документация может состоять как из одного руководства по процедурам, так и из нескольких.

5.2.3 Исполнение процедур

Для того чтобы иметь возможность выполнять процедуры, описанные в руководстве по процедурам, персонал должен о них знать, а также иметь возможность их выполнять, что часто достигается путем подготовки на специальных курсах либо в процессе повседневной работы.

Следует внедрить процедуры, обеспечивающие исполнение всеми использующими систему сотрудниками установленных требований.

5.2.4 Обновление и пересмотр

Важно обеспечить возможность определить, какие процедуры использовались в любой заданный момент времени на протяжении срока хранения любого конкретного информационного объекта. Такая возможность достигается поддержанием руководства по процедурам в актуальном состоянии и сохранением всех его предыдущих версий в соответствии с требованиями политики.

Любые изменения, вносимые в эксплуатационные процедуры, должны документироваться. Эта документация должна содержать сведения обо всех выполненных процедурах контроля изменений и о процедурах, обеспечивающих реализацию новых процедур на практике.

В случае реализации каких-либо изменений следует провести их проверку, с тем чтобы убедиться в том, что не нарушены эксплуатационные требования и требования политики.

Замененные версии руководства по процедурам должны храниться в соответствии с требованиями политики.

Для уверенности в актуальности документации необходимо регулярно проводить ее анализ и пересмотр. Такие пересмотры могут также оказаться необходимыми в случае внесения соответствующих изменений в законы или нормативные правовые акты.

Пересмотр документации должен проводиться как минимум раз в год, с тем чтобы обеспечить отражение в руководстве по процедурам всех изменений в процедурах и технологии.

Результаты периодических пересмотров должны документироваться и утверждаться лицами, ответственными за эксплуатацию соответствующих частей системы.

5.3 Сбор и включение в систему (capture) информации

5.3.1 Общие положения

Если доверенная система управления документами и информацией используется для хранения электронных объектов, то процедуры, используемые в процессе сбора и ввода в систему (захвата) этих объектов, должны быть задокументированы.

В число таких процедур могут входить процедуры:

- сбора и ввода в систему (захвата) электронных объектов;
- предварительной подготовки документов;
- формирования пакетов документов;
- фотокопирования;
- сканирования;
- контроля качества графических образов.

Документы могут быть как бумажными, так и на микроформах.

Подраздел 5.4 содержит более подробные сведения о процедурах, связанных со сканированием документов.

5.3.2 Потеря информации

В случае хранения электронных объектов в доверенной системе управления документами и информацией потенциально существует возможность потери части информации. Например, при сканировании бумажного документа разрешение может оказаться таким, что мелкие символы в электронном образе будут неразборчивыми; а в случае конверсии электронного документа из одного формата в другой могут быть потеряны некоторые метаданные.

В случае смены носителя информации физические доказательства (например, отпечатки пальцев на бумажных документах или компакт-дисках) могут не воспроизводиться в составе электронного объекта. В таких случаях организация должна проанализировать все потенциально возможные случаи потери информации и принять решение о том, является ли эта потеря приемлемой для делового процесса. Если такая потеря неприемлема, то необходимо принять меры, обеспечивающие сбор/захват и/или сохранение информации.

5.3.3 Создание и импорт электронной информации

Электронная информация может быть создана внутри доверенной системы управления документами и информацией или импортирована в нее. Ключевую роль играет аутентичность документов во время их создания или импорта, поскольку доверенная система управления документами и информацией в дальнейшем будет последовательно воспроизводить любую сохраненную в ней информацию.

Электронная информация может храниться в двух формах: в виде графических образов либо в виде объектов данных. В каждой из форм электронные объекты могут быть импортированы в доверенную систему управления документами и информацией в разнообразных форматах.

Графические образы, как правило, получаются:

- в результате обработки бумажных документов (оригиналы, фотокопии, факсы);
- путем автоматического приема факсимильных сообщений (через факс-сервер);
- путем создания копий экрана, на которых множество фрагментов информации отображается одновременно (их также относят к числу составных промежуточных документов — compound transient documents);
- в результате обработки микрофильмов и микрофиш.

Графические образы, как правило, являются растровыми представлениями оригинальных аналоговых документов. Они также могут быть получены путем преобразования цифровых документов. Особенности процедур захвата аналоговых документов в виде графических образов см. в 5.4.

Объекты данных используются для хранения информации в «первоначальном» (native) формате, при этом для извлечения содержащейся в них информации может потребоваться оригинальное программное обеспечение. Существует ряд «стандартных» форматов, с которыми могут работать многие программные пакеты (например, простые текстовые файлы, текстовые файлы табличных данных с разделителями). Примерами объектов данных являются:

- объекты, создаваемые офисными системами, такими как текстовые редакторы, электронные таблицы и т. д.;
- чертежи в системах автоматизированного проектирования;
- сообщения электронной почты;
- файлы, используемые в EDI-системах электронного обмена структурированной информацией;
- мгновенные сообщения;
- XML-сообщения;
- копии экрана (например, для создания промежуточных документов).

В любом случае к содержащейся в данных информации можно получить доступ с помощью подходящего программного приложения. Особенности процедур захвата аналоговых документов в виде объектов данных обсуждаются в 5.5.

Примечание — Электронные документы смогут представлять собой смесь данных и графических образов (примером может служить письмо в формате Word со встроенным растровым изображением подписи).

В тех случаях, когда информация, которая будет храниться в доверенной системе управления документами и информацией, поступает извне зоны контроля организации, использующей эту доверенную систему, возможности контроля и знания о процедурах и процессах, связанных с созданием и авторизацией этой информации, могут оказаться ограниченными либо отсутствовать. В этих обстоятельствах организации необходимо позаботиться о том, чтобы информация являлась именно тем, чем она претендует быть, чтобы в нее не вносились несанкционированные изменения и чтобы сведения об источнике информации соответствовали действительности. Степень проверки выполнения этих критериев будет зависеть от характера конкретной информации.

Такие пограничные ситуации могут также существовать и внутри организации. В этих случаях та часть организации, к которой относится доверенная система управления документами и информацией, не должна признавать графический образ или объект данных аутентичным только потому, что он поступил из другой части той же организации.

5.3.4 Метаданные

При создании или импорте электронных и/или аналоговых документов следует принимать меры, обеспечивающие передачу также всех соответствующих метаданных. Необходимо принять меры, гарантирующие сбор всех необходимых метаданных, с тем чтобы обеспечить правильную интерпретацию электронных и/или аналоговых документов.

Возможно, придется провести анализ содержащейся в метаданных информации на полноту и адекватность. Наличие полного набора метаданных с адекватным содержанием увеличивает доказательную силу той информации, к которой он относится. Следует рассмотреть возможность использования подходящих схем метаданных.

5.4 Создание и включение в систему (capture) графических образов документов

5.4.1 Общие положения

Настоящий подраздел содержит рекомендации, касающиеся процедур, имеющих отношение к созданию электронных графических образов аналоговых документов. Рекомендации данного подраздела предназначены для пользователей, чьи доверенные системы управления документами и информацией включают в себя возможности ввода и сохранения аналоговых документов в электронном виде с использованием сканеров. Эти рекомендации охватывают следующие процедуры:

- подготовка документов к сканированию;
- формирование пакетов;
- фотокопирование;
- сканирование;
- обработка изображений.

5.4.2 Подготовка бумажных документов к сканированию

Перед сканированием следует изучить все бумажные документы, с тем чтобы обеспечить получение качественных графических образов. Такие характеристики, как размер, масса и брошюровка, цвет бумаги и отпечатанного текста, могут повлиять на физический процесс сканирования.

Изучение бумажных документов должно проводиться до начала процесса сканирования, с тем чтобы убедиться в их пригодности к сканированию. Процедуры этого процесса изучения должны быть задокументированы.

Следует принять во внимание такие факторы, как физическое состояние документов (бумага тонкая, мятая, со скрепками, и т. д.) и информационные свойства (изображение черно-белое, цветное, диапазон тональности и т. д.).

В тех случаях, когда выяснится, что бумажные документы вряд ли будут приняты сканером, можно воспользоваться рядом технических приемов. Например, можно сначала сделать фотокопию оригинала или поместить его при сканировании в прозрачный конверт.

Процедуры работы с теми бумажными документами, которые могут вызвать трудности при сканировании, должны быть задокументированы. При удалении скоб, скрепок и других средств брошюровки бумажных документов следует позаботиться о том, чтобы оригиналу не был причинен ущерб, способный повлиять на качество захвата содержащейся в документе информации.

Если бумажный документ имеет физические приложения, например, записки на стикерах, то система должна предоставлять средства, позволяющие отличать их от документа, к которому они прикреплены.

Этого можно добиться, например, путем захвата отдельного графического образа приложения вместе с соответствующими данными, позволяющими связать его с исходной страницей. Если захватывается один образ страницы вместе с находящимся на ней приложением, то в метаданных можно задокументировать факт наличия приложения. Если существует риск того, что физическое приложение перекроет (или будет казаться, что оно перекрывает) часть информации в бумажном документе, то может оказаться предпочтительным обеспечить также захват графического образа бумажного документа без приложения.

Если в бумажный документ внесены физические правки, например, с использованием белой непрозрачной краски, то система должна обеспечить, чтобы наличие таких правок было отмечено.

Процедуры, используемые при сканировании многостраничных бумажных документов, скрепленных с помощью скоб, скрепок или зажимов, должны быть задокументированы.

Все страницы многостраничных документов следует хранить вместе и в соответствующем порядке до, во время и после сканирования.

5.4.3 Формирование пакетов документов

Там, где возможно, бумажные документы для сканирования следует группировать в пакеты.

Группировка в пакеты упрощает контроль над бумажными документами и дает возможность осуществлять контроль качества и другие процедуры на выборочной основе.

Объем пакета следует выбирать из соображений удобства.

Число бумажных документов в пакете будет зависеть от конкретных обстоятельств. Например, если документы помещены в папки и среднее число документов в одной папке достаточно велико (например, 100 страниц), то документы из одной папки могут рассматриваться как пакет. Если папки содержат относительно небольшое число документов (например, в среднем 10 страниц), то пакет может формироваться из документов нескольких папок. Если обрабатываются документы на рулонных микропленках, то один рулон пленки может рассматриваться как пакет.

Объем пакета следует выбирать так, чтобы он не превышал объема, которым можно легко управлять, но и не был слишком мал, с тем чтобы выборочный контроль качества на уровне пакетов не приво-

дил к существенному снижению эффективности всего процесса. Объем выборки, возможно, потребуется определять с использованием методов выборочных статистических испытаний.

В ряде прикладных задач непросто четко выделить пакеты. В этих случаях пакет может определяться как массив бумажных документов, поступивших на вход в течение определенного периода времени. Например, пакетом могут считаться все документы, поступившие на обработку в течение одного часа или одних суток.

В ряде приложений (особенно в приложениях, реализующих workflow-процессы), в которых нельзя использовать разделение на пакеты, следует применять альтернативные методы, обеспечивающие сканирование всех бумажных документов. В число таких методов может входить маркировка документов после сканирования или дополнительная проверка путем сопоставления графических образов с бумажными оригиналами.

5.4.4 Фотокопирование

Некоторые бумажные документы перед сканированием полезно фотокопировать. К таким документам относят:

- документы, на которые может негативно повлиять процесс сканирования, например, поврежденные или хрупкие документы;

- документы, отличающиеся существенными вариациями плотности и контраста оригинала, если фотокопирование позволяет заметно улучшить качество изображения;

- документы, использующие бумагу или чернила таких цветов, при сканировании которых не удается получить разборчивых графических образов.

Примечание — Фотокопиры и сканеры могут по-разному реагировать на различные цвета, но лишь в исключительных случаях метод предварительного фотокопирования перед сканированием не позволяет получить удовлетворительных результатов;

- сложенные документы, которые слишком велики для того, чтобы сканировать их целиком в один полноразмерный графический образ.

Примечание — При фотокопировании могут быть созданы уменьшенные изображения, которые затем сканируют; и/или с оригинала либо с его фотокопий может быть получено несколько отсканированных графических образов.

Фотокопии следует проверять для того, чтобы гарантировать отсутствие существенной потери информации в ходе процесса фотокопирования.

Если бумажные документы предварительно перед сканированием фотокопируются, то используемые при этом процедуры должны быть задокументированы в руководстве по процедурам.

Для того чтобы гарантировать отсутствие потерь какой-либо существенной информации в процессе сканирования отфотокопированных бумажных документов, следует внедрять дополнительные процедуры контроля качества.

Если при фотокопировании изображение было уменьшено, то следует выполнить проверки на отсутствие связанных с уменьшением эффективного разрешения изображения существенных потерь мелких деталей в отсканированных графических образах по сравнению с бумажными оригиналами.

При создании на основе одного документа нескольких графических образов эти образы должны взаимно перекрываться, с тем чтобы гарантировать отсутствие существенной потери информации на стыках между соседними графическими образами.

Если графический образ создается на основе фотокопии, то это должно быть ясно для пользователя изображения. Также должно быть ясно, была ли фотокопия снята с бумажного документа при его подготовке к сканированию или бумажный документ изначально представлял собой фотокопию. Ясность в этом вопросе необходима для того, чтобы графический образ мог быть правильно идентифицирован как точная факсимильная копия бумажного документа, даже если в ходе процедур предварительной подготовки была снята промежуточная фотокопия, а также для различения таких графических образов и графических образов, полученных на основе фотокопий, сделанных при неизвестных обстоятельствах.

Решить данную задачу можно, например, на этапе подготовки документов к сканированию, путем проставления штампов или маркировки сканируемого материала как промежуточной фотокопии или документа, изначально имевшгося в виде фотокопии, либо при помощи электронной маркировки полученных с фотокопий графических образов, различая при этом промежуточные фотокопии, сделанные в ходе подготовки документов к сканированию, и бумажные документы, изначально имевшиеся в виде фотокопий.

Процедуры, применяемые в случаях, когда неизвестно, является ли бумажный документ оригиналом или фотокопией, должны быть задокументированы.

5.4.5 Процессы сканирования

Подробные сведения о процедурах, применяемых при сканировании аналоговых документов, должны быть включены в руководство по процедурам.

Все варианты процедур сканирования, связанные с типом сканируемого документа, должны быть подробно описаны в руководстве по процедурам.

Подобные варианты могут применяться, например, в случаях сканирования двусторонних бумажных документов в отличие от односторонних, а также цветных изображений в отличие от черно-белых.

Процедуры должны обеспечивать, чтобы все бумажные документы пакета были полностью отсканированы; ни один документ не должен остаться неотсканированным.

Для проверки того, что все бумажные документы были отсканированы, число обработанных документов может сравниваться с числом документов в пакете. Если разделение на пакеты не используется, то могут потребоваться альтернативные процедуры, обеспечивающие сканирование всех документов.

Если важно, чтобы все страницы многостраничного бумажного документа были отсканированы, то должны быть реализованы процедуры, обеспечивающие выполнение этого требования.

Для каждого бумажного документа число полученных при его обработке графических образов можно сравнить с числом страниц (т. е. сторон листа), принимая также во внимание процессы удаления пустых (или каких-либо иных) страниц. Однако ошибки при ручном подсчете физических бумажных документов и содержащихся в них страниц могут сделать подобный процесс неэффективным. Удовлетворительным решением может быть внедрение процедур, обеспечивающих приемлемо малую вероятность и риск несканирования/не полного сканирования какого-либо документа. Этот риск следует оценить и, где это необходимо, провести пересмотр процедур на предмет уменьшения данного риска.

Многие сканеры снабжены устройствами автоматической подачи бумажных документов, способными надежно детектировать неправильную подачу, минимизируя тем самым риск того, что документ пройдет через сканер, но не будет отсканирован. Если подобные устройства не используются, то необходимы процедуры, обеспечивающие ручную обработку каждого документа оператором сканера, с тем чтобы уменьшить вероятность того, что какой-либо документ не будет отсканирован.

Если критически важно обеспечить сканирование каждого листа, то пользователям следует рассмотреть возможность подсчета или предварительной индексации бумажных документов, с тем чтобы точно определить число страниц в документе или пакете документов.

Использование метода «двойного ввода» может обеспечить очень высокую точность определения числа страниц. Впоследствии эти данные могут быть сопоставлены с числом отсканированных страниц; любая недостача будет указывать на то, что либо произошла подача одновременно нескольких страниц, либо какая-то страница была неправильно перемещена после предварительной индексации и перед сканированием.

Если для сканирования двусторонних документов используется односторонний сканер (т. е. способный одновременно сканировать только одну строну бумажного документа), то следует принять меры, обеспечивающие переворачивание каждого двустороннего документа и сканирование обратной стороны.

Если большой бумажный документ сканируют по частям и при этом создается несколько графических образов, то эти части должны перекрываться, чтобы исключить возможность потери информации на стыках между соседними графическими образами.

Система сканирования должна поддерживать возможность уникальной идентификации каждого электронного документа, причем так, чтобы эта идентификация не могла быть изменена или удалена, за исключением случаев, в которых это допускается в соответствии с 6.11.

Эта уникальная идентификация может представлять собой создаваемой системой сканирования порядковый номер, который может использоваться только для целей внутреннего контроля.

5.4.6 Контроль качества

5.4.6.1 Тестовый набор документов (sample set)

Необходимы процедуры, снижающие риск получения отсканированных графических образов неудовлетворительного качества. Доказывать аутентичность проще, если может быть показано, что графические образы хорошего качества и что сканер во время сканирования работал в соответствии с установленными требованиями.

Для оценки соответствия результатов работы сканера установленным критериям контроля качества следует подготовить тестовый набор бумажных документов. Документы тестового набора должны быть репрезентативным отражением всего массива подлежащих сканированию документов. В число документов тестового набора следует включать образцы бумажных документов более низкого по сравнению с большинством документов качества.

Критерии контроля качества могут охватывать:

- общую читаемость/разборчивость;
- разборчивость мельчайших деталей в полученных графических образах (например, шрифта наименьшего размера для текста, разборчивость знаков препинания, в том числе десятичной точки);
- полноту деталей (например, приемлемость искаженных символов, отсутствие фрагментов линий);
- точность передачи размеров по сравнению с оригиналом;
- наличие порожденных сканером точек и пятен (отсутствующих в оригинале);
- полноту графического образа в целом (то есть отсутствие утраты информации по краям графического образа);
- плотность сплошных черных зон;
- точность цветопередачи.

Критерии контроля качества графических образов должны быть реалистичными, учитывая характер исходного материала и характеристик сканирующего оборудования.

Критерии контроля качества, используемые для контроля качества отсканированных графических образов, должны быть задокументированы. Эти критерии должны быть согласованы со всеми заинтересованными сторонами, включая внутренних и внешних пользователей, для которых качество графических образов с большой вероятностью может повлиять на возможность их использования.

Критерии контроля качества должны основываться на использовании тестового набора бумажных документов.

5.4.6.2 Оценка качества графического образа

Процедуры, определяющие процесс, повседневно используемый для оценки качества графических образов, должны быть задокументированы.

Процедуры оценки качества графических образов должны содержать подробные сведения о порядке оценки результатов сканирования, включая характеристики устройства для поиска и отображения графических образов.

При оценке результатов процедуры контроля качества следует проявлять осторожность. Полученные результаты могут зависеть от конкретных устройств вывода (таких как монитор или принтер).

Если в процедурах контроля качества будет использоваться принтер, то разрешение принтера должно быть не ниже, чем разрешение отсканированных графических образов.

В тех ситуациях, когда это имеет значение, принтер должен быть способен точно воспроизводить цвета или оттенки серого цвета.

Если качество воспроизведения цвета или оттенков серого цвета имеет значение, то следует провести оценку точности воспроизведения цвета или оттенков серого цвета.

Если точность передачи размеров имеет важное значение, то должны быть задокументированы процедуры проверки того, что размеры воспроизводятся в пределах допустимых отклонений. Такие процедуры могут, например, включать в себя проверку точности номинального разрешения сканера, с тем чтобы размеры в графическом образе можно было определить путем подсчета числа пикселей между определенными точками изображения.

Если качество графических образов во время выполнения процедур сканирования проверяет оператор сканера, то должна выполняться вторая процедура контроля качества, проводимая иным персоналом, чем персонал, отвечающий за сканирование. В ходе второй проверки качества могут применяться методы выборочных статистических испытаний.

Процедуры контроля качества должны быть взаимосвязаны с процессом обработки пакетов (если используется) в соответствии с 5.4.3, что позволяет принимать или отвергать пакет независимо от других пакетов.

Результаты всех проверок, проводимых при контроле качества, должны сохраняться в протоколе (журнале) контроля качества (quality control log), который может вестись вручную или автоматически.

В workflow-среде автоматизации выполнения рабочих процессов, в которой каждый электронный документ рассматривается в рамках workflow-процесса, в случае, если имеются операции явной проверки качества графических образов и отбраковки образов неприемлемого качества, эти операции могут рассматриваться как процесс контроля качества.

Если процедуры контроля качества предусматривают создание выборок отсканированных графических образов и других взаимосвязанных данных, то нет необходимости жестко фиксировать размер выборки, который может изменяться в зависимости от частоты возникающих проблем и характера исходного материала. Для определения подлежащего проверке процента отсканированных графических образов следует использовать (где это уместно) методы выборочных статистических испытаний. Более подробные сведения о выборочном контроле см. в ГОСТ Р ИСО 2859-1.

В большинстве случаев проверять весь обработанный материал непрактично, поэтому, как правило, проверяют только часть обработанного материала. Например, в начале сканирования могут проверяться выборки относительно большого (например, 20 %) объема, который впоследствии может быть уменьшен (например, до 10 % или даже до 5 %) по мере того, как демонстрируется устойчивое соответствие заданным критериям качества.

Если при контроле качества используется выборочная проверка отсканированных графических образов, то должна быть задокументирована частота отбора образцов.

5.4.6.3 Проверка работоспособности сканера

С целью мониторинга системы и проверки ее функционирования в пределах допустимых отклонений следует периодически проводить проверки работоспособности сканера.

Для определения соответствия критериям качества могут быть распечатаны отсканированные графические образы тестовых мишеней и сопоставлены с самими тестовыми мишенями согласно приведенному в процедурах описанию.

Использование тестовых мишеней дает возможность объективно оценить и измерить качество работы сканера. Регулярное их использование может показать, работает ли сканер устойчиво и в соответствии с его спецификациями. Для такой оценки может использоваться тестовая мишень, приведенная в ИСО 12653-2.

Частота проверок работоспособности сканера должна определяться загруженностью системы и учитывать ожидаемое ухудшение работоспособности системы. Для этого могут понадобиться рекомендации поставщика системы, а также опыт ее использования. Первоначально целесообразно сканировать тестовую мишень после сканирования каждых нескольких тысяч страниц.

Если используются двусторонние (дуплексные) сканеры, то предпочтительно использовать двусторонние тестовые мишени. Односторонние тестовые мишени могут быть использованы для проверки дуплексных сканеров только в том случае, если невозможно получить двусторонние тестовые мишени.

Тестовые мишени не являются адекватным представлением реально сканируемых бумажных документов, и их не следует рассматривать в качестве замены тестового набора документов.

5.4.7 Повторное сканирование (rescanning)

Процедуры повторного сканирования бумажных документов должны быть задокументированы. Повторное сканирование может потребоваться, если полученный первоначально графический образ был забракован из-за его плохого качества или по иным показателям.

Следует внедрить процедуры, обеспечивающие замену забракованного графического образа на образ, полученный в результате повторного сканирования, а также отсутствие компрометации процедур нумерации пакетов и сбора контрольной информации (audittrailprocedure).

5.4.8 Обработка графических образов

Методы обработки графических образов, применяемые для улучшения качества изображения, должны быть описаны в руководстве по процедурам.

Если возможно использование контролируемых оператором средств, то должны быть задокументированы сведения о том, какие именно средства использовались для обработки конкретных электронных документов.

5.5 Сбор и включение в систему (capture) данных

5.5.1 Новые данные

Данные (например, для создания индекса или другой справочной информации) могут вводиться/захватываться с существующих аналоговых и/или электронных документов и вводиться в компьютер с использованием ряда способов, включая ручной (т. е. ввод непосредственно с клавиатуры), автоматизированный [(например, путем считывания штрих-кода, чтения оптических меток (Optical Mark Reading, OMR), оптического/интеллектуального распознавания символов (OCR/ICR)] и полуавтоматический (скажем, когда данные, собранные автоматически, например, с использованием оптического распознания символов, подтверждаются с помощью ручного повторного ввода). В каждом случае необходимо обеспечить уверенность в правильности введенных данных. На практике может оказаться сложно или вообще невозможно обеспечить 100 %-ную точность вводимых данных, и пользователю необходимо оценить риск, связанный с наличием ошибок.

Если внешние данные собираются с целью последующего ввода в систему, то следует установить требуемые уровни качества. Эти уровни качества должны отражать точность и полноту собранных/захваченных данных.

Устанавливаемые уровни точности могут варьироваться в зависимости от прикладной задачи и важности каждого конкретного элемента данных.

Следует определить процедуры проверки выдерживания уровней точности. Такие процедуры, как правило, основаны на случайной или псевдослучайной выборке пакетов собранных данных и проведении их сопоставления с исходным материалом. Как правило, пакеты, не соответствующие требуемым уровням точности, отправляют на повторную обработку, и ее результаты еще раз проверяют, чтобы обеспечить выдерживание требуемых уровней точности.

Результаты всех проверок точности должны документироваться.

Если данные извлекают из электронного документа, то оригинальный документ следует сохранить, связав его с извлеченными данными.

5.5.2 Конверсия и миграция

Если данные поступают из другой системы (или части системы) в ходе миграции системы хранения данных, то необходимо разработать, внедрить и задокументировать используемые при этом процедуры и процессы.

Если проводится конверсия информации из текущего в новый файловый формат, то следует задокументировать все потенциальные возможности потери информации вследствие выполнения этого процесса [в том числе контрольной информации (audit trail)].

5.6 Индексирование

5.6.1 Общие положения

Индексирование (индексация) является важнейшей частью процесса сохранения информации на электронных носителях, поскольку она дает возможность получить доступ к соответствующей информации. В случае утраты индексирующей информации сохраненная информация также может быть утрачена.

Индексирование может выполняться автоматически (т. е. системой без вмешательства оператора) или вручную. В случае ручного индексирования важно обеспечить исполнение соответствующих документированных процедур.

Некоторые системы дают возможность при вводе/захвате информации сохранить частичную индексирующую информацию, которая впоследствии может быть объединена с дополнительной индексирующей информацией, введенной вручную.

Процедуры и правила индексирования сохраняемой информации должны быть задокументированы.

5.6.2 Ручное индексирование

Ручное индексирование предусматривает визуальное изучение вводимой в систему информации либо до ее ввода, либо в рамках процессов, выполняемых после ввода.

Сотрудники, занимающиеся ручным индексированием, должны получать специальную подготовку с целью обеспечения максимальной точности индексирования. Требования и процедуры профессиональной подготовки по индексированию должны быть задокументированы.

5.6.3 Автоматическое индексирование

Автоматическое индексирование может осуществляться, например, путем считывания штрих-кодов или использования методов оптического распознавания символов. В случае использования автоматического индексирования процедуры проверки и корректировки неточной индексирующей информации должны быть задокументированы.

5.6.4 Сохранение индексирующей информации

Индексирующая информация должна сохраняться в течение срока, не меньшего, чем срок хранения информации, к которой она относится.

Некоторые системы требуют проведения периодического перестроения индексов баз данных, обычно с целью улучшения производительности базы данных. Процедуры перестроения индексов должны быть задокументированы.

5.6.5 Корректировка индексирующей информации

Процессы индексирования могут включать в себя процедуры по обнаружению недостающей информации. При индексировании отображаемой информации отсутствующий материал удается обнаружить, только если сравнивать отображаемую информацию с оригиналами или при упорядочении информации (например, с использованием последовательной нумерации).

Процедуры изменения и/или корректировки индексирующей информации должны быть задокументированы. В случае внесения исправлений в запись индекса, возможно, потребуется сохранить сведения о содержании индекса до и после внесения изменений.

Если запись в индексе относится к удаленной или уничтоженной информации, то сведения об этом следует сохранить.

В тех случаях, когда во исполнение законодательно-нормативных требований может потребоваться проведение удаления или уничтожения хранимой информации путем изменения или удаления записей в индексе, соответствующие процедуры должны быть задокументированы.

5.6.6 Точность индексирующей информации

Индексирующие данные для отсканированных изображений могут быть неточными. В то время как точное индексирование упрощает поиск и извлечение хранимой информации, точность соответствующих индексирующих данных указывает на ее актуальность и полноту, тем самым подтверждая аутентичность хранимой информации. И наоборот, неточность индексирующих данных может привести к тому, что пользователь не сможет извлечь нужную либо получит ненужную информацию.

Критерии точности индексирующей информации могут варьироваться в зависимости от целевой задачи. В некоторых случаях точность может быть задана как максимально допустимое число ошибочных символов на тысячу символов введенной информации (или как эквивалентный процент числа введенных символов). В других случаях точность может быть задана как максимально допустимое число слов (или других наборов символов, таких, например, как номер клиента или детали), содержащих какие-либо ошибки (в одном или нескольких символах).

Критерии уровней точности индексирующей информации должны быть реалистичными, с учетом использованного метода сбора и ввода индексирующих данных, типичной частоты случайных ошибок при работе персонала, занимающегося вводом данных, и читаемости исходного материала. Уровни точности могут варьироваться в зависимости от типа индексируемой информации.

В случае, если выполняется ручная или автоматическая индексация, должны быть согласованы и задокументированы уровни точности. Должны быть также задокументированы процедуры проверки точности индексирующей информации.

5.7 Процедуры создания заверенных копий электронной информации (authenticated output procedures)

Может возникнуть необходимость представить выдачу из электронных систем хранения в виде бумажных копий либо в виде электронных объектов на соответствующих носителях для использования в качестве документальных доказательств. Как правило, такие копии должны быть заверены в соответствии с установленными требованиями как точные копии оригинала, с тем чтобы уменьшить вероятность их непринятия или оспаривания.

Следует задокументировать процедуры создания копии хранимой информации, которые могут понадобиться в качестве документальных доказательств. Такие процедуры могут, например, предусматривать использование стандартных средств копирования системы и создание авторизованным лицом письменного подтверждения того, что процесс копирования был выполнен корректно. В процедурах может быть указано, как впоследствии следует обращаться с этими копиями. Процедуры могут ссылаться на контрольную информацию (audit trail data) для подтверждения процессов, происходивших во время копирования.

Если бумажная копия создается как часть выдачи, то процедуры должны включать в себя подписание копии уполномоченным лицом или иную процедуру подтверждения точности копии.

Важно осознать характер и масштабы всех изменений, вносимых средствами извлечения, и оценить их значение. То, что приемлемо при обычном применении, может оказаться неприемлемым в иных обстоятельствах, когда выдачу из системы требуется использовать в качестве доказательств, например:

- черно-белое отображение цветного графического образа может быть приемлемо в ситуациях, когда цвет не имеет значения, однако в иных обстоятельствах цвет может иметь ключевое значение, что потребует применения иных средств отображения;

- просмотр графического образа в более низком разрешении, чем использованное при сканировании оригинальных бумажных документов, может быть приемлемым при повседневной работе, однако мелкие детали, которые при этом теряются, могут быть важны, когда, например, они могут иметь значение для судебной экспертизы;

- в случае отсутствия точного соответствия между разрешением отсканированного графического образа и разрешением устройства отображения возможна потеря точности передачи размеров у воспроизведенного графического образа;

- если сохраненный файл данных для просмотра или печати обычно преобразуется в другой формат, то информация может быть потеряна или представлена в иной форме в связи с потерей деталей и различиями в расположении элементов (layout). Эти различия могут оказаться неприемлемыми для целей раскрытия/представления информации, и в этих случаях могут понадобиться иные средства вывода, не требующие проведения конверсии.

Если средства системы, используемые для извлечения, показа и/или печати хранящейся информации, не поддерживают форматирование оригинала (например, шрифты, разбиение на страницы), то следует согласовать и задокументировать характеристики выводимой информации.

5.8 Передача файлов

5.8.1 Внутрисистемная передача файлов данных

5.8.1.1 Общие положения

Внутрисистемной (intra-system) является передача файлов, происходящая внутри системы, в соответствии с 6.2. Примерами внутрисистемной передачи файлов являются:

- передача по локальной сети;
- перемещение между контролируемыми системой подсистемами хранения, например, в иерархической системе управления хранением данных или между кэш-памятью и магнитным диском;
- передача между подсистемами хранения под контролем оператора.

При такой передаче как электронные, так и ручные процедуры находятся под контролем организации.

Следует внедрять процедуры и процессы, обеспечивающие отсутствие компрометации целостности передаваемых внутри системы файлов.

Передача файлов с одного устройства на другое должна контролироваться прикладным программным обеспечением.

Если необходимы дополнительные меры безопасности, следует рассмотреть возможность использования электронных цифровых подписей.

Примечание — Требования настоящего подраздела не распространяются на миграцию файлов, при которой тип носителя и/или формат файла данных могут изменяться по причинам, обусловленным технологией миграции (см. 6.10).

5.8.1.2 Передача по локальной сети

В некоторых приложениях файлы могут быть переданы под контролем оператора с одного устройства хранения на другое с помощью локальной сети в соответствии с 6.2. Локальные сети могут включать в себя соединения между удаленными пунктами с использованием наземных линий (fixedlines).

Если файлы передаются через локальную сеть, то следует внедрять процедуры и процессы, обеспечивающие отсутствие компрометации целостности передаваемых файлов.

Если файлы передаются между удаленными пунктами по наземным (например, арендованным) линиям связи, то следует внедрять процедуры и процессы, обеспечивающие отсутствие компрометации целостности передаваемых файлов.

5.8.2 Передача файлов во внешние системы

В настоящем пункте речь идет о файлах, передаваемых между двумя системами с использованием внешних (глобальных) коммуникационных систем. Такие системы являются внешними по отношению к системе, описанной в разделе 6. Отправляющая и получающая системы удалены друг от друга и могут принадлежать как той же, так и различным организациям; в любом случае услуги по передаче предоставляет другая сторона.

Коммуникационная система может использовать как передачу в режиме реального времени, так и отложенную передачу (сохранение и последующая пересылка), как это происходит в системах электронной почты.

В настоящем стандарте рассматривается целостность электронных объектов, передаваемых другой стороне, а также целостность электронных объектов, получаемых от другой стороны. В настоящем стандарте вопросы, связанные с оказанием услуг по передаче, прямо не рассматриваются. Следуя требованиям настоящего стандарта, пользователи могут показать, что копия электронного объекта, переданного в некоторый предшествующий момент времени другой стороне, не была с тех пор изменена и что файл, полученный в некоторый предшествующий момент времени от другой стороны, с момента получения не был изменен.

Передача файлов с одного устройства на другое должна контролироваться прикладным программным обеспечением.

Если другой стороне передается копия файла, то исходный файл должен быть сохранен в системе.

Дата и время всех передач файлов должны сохраняться в составе контрольной информации (audittrail).

Если файл получен от другой стороны посредством передачи, то его следует сохранить в системе.

Дата и время получения любых файлов должны сохраняться в составе контрольной информации (audittrail).

Различия между переданными и полученными файлами могут быть вызваны ошибками при передаче или преднамеренным изменением одного из этих файлов. То, что посланный и полученный файлы содержат идентичные данные, доказывается так же, как эквивалентность любых двух копий. Первоочередная потребность заключается в том, чтобы показать, какой файл является первоисточником, а какой — копией, т. е. какой из файлов был создан первым. В ряде случаев этот вопрос может быть решен путем сопоставления времени сохранения файлов. Если часы системы точны (учитывая различия в часовых поясах), полученный файл должен был быть сохранен в более поздний момент времени по сравнению с передававшимся файлом. Таким образом, установление первоисточника сводится к способности доказать надежность и точность определения времени двух событий.

Электронные/цифровые подписи, например, могут быть использованы для подтверждения того, что подписанный электронной/цифровой подписью документ является точно таким же, каким он был отправлен, а также для удостоверения личности отправителя. Такое подтверждение личности может быть скомпрометировано в случае, если первоначальный сертификат стал недействительным и уже не поддерживается удостоверяющим центром. Если сертификат электронной/цифровой подписи более не доступен или срок его действия истек, то электронная цифровая подпись позволит только узнать, был ли документ модифицирован с момента подписания.

Из соображений безопасности и по иным причинам могут быть реализованы дополнительные процедуры (выходящие за рамки рассматриваемых в настоящем стандарте), например, для предотвращения несанкционированного раскрытия содержащейся в файле информации.

Если важно иметь возможность доказать факт доставки файла, то отправитель может потребовать, чтобы принимающая система передала отправителю подтверждение доставки, которое должно включать в себя идентификатор передачи и дату и время доставки.

Если эти процедуры выполняются, то снижается риск того, что файл был изменен или был послан не указанным отправителем, а иным лицом.

Следует также оценить уровень риска безопасности при внешней передачи файлов, с тем чтобы обеспечить соответствие требованиям политики информационной безопасности.

5.9 Сохранение бумажных документов (document retention)

Если бумажные документы сканируются и при этом политика в области управления документами и информацией устанавливает, что общим правилом является последующее уничтожение бумажных документов данного вида, то возможны случаи, при которых следует сделать исключение и сохранить бумажный документ. Следует отметить, что в случае сохранения «оригинального» бумажного документа может понадобиться получить к нему доступ с целью подтверждения аутентичности электронной «копии».

Следует задокументировать процедуры, идентифицирующие конкретные бумажные документы, которые необходимо сохранить.

В число обстоятельств, при которых может потребоваться сохранить бумажный документ, входят следующие обстоятельства:

- низкое качество бумажного документа, из-за чего невозможно получить его разборчивый графический образ;

- необходимость снизить риск быть обвиненным в том, что графический образ был умышленно сделан неразборчивым. Сохранение бумажного документа позволяет также избежать риска отказа в приеме графического образа в качестве доказательства на том основании, что он не является точной копией бумажного документа;

- ввиду низкого качество оригинального бумажного документа сохраняется записка, констатирующая данный факт и детально описывающая и документирующая плохо видимую информацию во избежание ее утраты;

- бумажный документ содержит физические (механические) поправки и подчистки (например, с помощью корректурных жидкостей и коррекционных лент) или физические аннотации (например, на стикерах), которые сложно идентифицировать в отсканированном графическом образе;

- в бумажном документе имеются физические (механические) поправки и подчистки и физические аннотации, и считается достаточным создать отдельный документ, содержащий подробные сведения о том, что представляли собой эти поправки, подчистки и аннотации;

- выявлено мошенничество либо начато или ожидается судебное разбирательство или расследование, к которым имеет отношение конкретный бумажный документ;

- бумажный документ имеет большую ценность, например, подписанный оригинал крупного контракта.

Следует задокументировать процедуры выявления информации, относящейся к обнаруженному мошенничеству либо к начатому или ожидаемому судебному разбирательству или расследованию. Такие процедуры должны включать в себя приостановление исполнения политики уничтожения бумажных документов в отношении этой информации.

5.10 Обеспечение долговременной сохранности информации

Следует задокументировать процедуры обеспечения долговременной сохранности информации. Такие процедуры должны учитывать требуемые сроки хранения и ожидаемый срок службы систем хранения данных. Если срок хранения превышает ожидаемый срок существования систем хранения данных, то необходимо задокументировать планы миграции в новые системы (см. также 6.10). Дополнительную информацию см. в ISO/TR 18492.

5.11 Уничтожение информации

Процедуры уничтожения или удаления информации по истечении срока хранения должны быть задокументированы.

Эти процедуры должны включать в себя меры безопасности, соответствующие степени конфиденциальности уничтожаемой информации.

Бумажные документы не должны уничтожаться до тех пор, пока их графические образы не будут успешно записаны на устройства хранения и не завершатся соответствующие процедуры резервного копирования[1)].

5.12 Резервное копирование и восстановление системы

Следует внедрить эффективные процедуры резервного копирования файлов, предусматривающие создание по крайней мере двух актуальных копий для использования в случае утраты или повреждения всей рабочей копии данных (livedata) или ее части. Крайне важно, чтобы резервные копии включали в себя и всю взаимосвязанную информацию (например, индексные файлы, контрольную информацию), с тем чтобы в случае полной утраты исходной системы можно было воссоздать заново законченную систему.

Такие процедуры должны предусматривать защищенное удаленное хранение этих резервных копий.

Процедуры восстановления системы также необходимо задокументировать, с тем чтобы продемонстрировать, что эти процедуры контролируются и проверяются на надежность.

Вопросы, связанные с безопасностью резервных копий, могут быть важны в случае спора по поводу аутентичности. Возможны обвинения в том, что резервные носители информации были скомпрометированы, а впоследствии использованы для восстановления после потери информации, повлияв таким образом на аутентичность хранимой информации. В некоторых случаях наличие защищенных хранящихся резервных копий, предназначенных для использования только в случае оспаривания аутентичности рабочих данных, может обеспечить возможность доказать аутентичность хранимой информации.

Имеющиеся в системе средства должны поддерживать возможность периодического проведения резервного копирования и проверки всех файлов и связанной с ними информации, включая контрольную информацию (audit trails).

Сведения обо всех проблемах, возникающих при выполнении процедуры, должны сохраняться в составе системной контрольной информации обо всех операциях резервного копирования.

Если структура файлов, сохраняемых на резервной копии, отличается от структуры оригиналов, то структура файлов резервной копии должна быть подробно описана в руководстве по системе (systems description manual).

Контрольная информация должна включать в себя подробные сведения обо всех операциях по восстановлению файлов, а также сведения обо всех проблемах, возникших во время выполнения процедур восстановления с резервных копий.

Следует задокументировать процедуры проверки того, что целостность файлов не была скомпрометирована в результате восстановления с резервных копий.

В случае, если резервные копии используются для восстановления после сбоя системы, процедуры следует задокументировать для обеспечения того, чтобы целостность файлов не была скомпрометирована.

[1)] Речь идет о документах с еще не истекшими сроками хранения, бумажные оригиналы которых допускается заменять электронными копиями.

Носители информации, используемые для хранения резервных копий, не обязательно подходят для постоянного хранения. Поставщики носителей информации обычно предоставляют сведения о рекомендуемой частоте тестирования носителей. Если такой конкретной информации не имеется, то в качестве альтернативы рекомендации общего плана часто можно найти в национальных или международных стандартах.

Тестирование носителей информации на одном и том же оборудовании не гарантирует того, что носители можно будет прочитать на других устройствах (даже того же поставщика и той же модели). Резервные копии не будут иметь ценности в случае, если будет утрачено то единственное оборудование, которое способно их прочитать.

Носители информации, используемые для хранения резервных копий, следует регулярно тестировать, используя для их чтения различное оборудование.

5.13 Техническая поддержка (maintenance) системы

5.13.1 Общие положения

Доверенная система управления документами и информацией должна поддерживаться, и техническая поддержка, связанная с устранения неполадок, должна выполняться только квалифицированным персоналом во избежание такого ухудшения работоспособности системы, которое могло бы повлиять на целостность созданных, введенных или сохраненных в системе данных.

Например, для систем сканирования бумажных документов особое значение имеет техническая поддержка в соответствии со спецификациями поставщика для поддержания качества получаемых графических образов.

Профилактическое обслуживание должно проводиться регулярно в соответствии с рекомендациями поставщика.

Процедуры, используемые для профилактического обслуживания, должны быть задокументированы.

Эти процедуры могут выполняться операторами системы или персоналом специализированной службы.

Следует вести журнал технического обслуживания (maintenance log), в котором фиксируются проведенные профилактические и корректирующие процедуры технического обслуживания.

Следует задокументировать процедуры контроля за использованием оборудования и/или программного обеспечения для технического обслуживания системы, которые способны обойти меры и средства системы по контролю и управлению доступом. Доступ к таким инструментам и средствам должен строго контролироваться и отслеживаться.

Информацию о времени простоя системы и подробные сведения о принятых мерах следует фиксировать в журнале технического обслуживания.

5.13.2 Системы сканирования

Если реализовано сканирование бумажных документов, то процедуры, описанные в разделе, посвященном контролю качества (см. 5.4.6), должны использоваться для проверки того, что по завершении процедур технического обслуживания сканирующая система продолжит обеспечивать требуемое качество графических образов.

Впоследствии результаты тестирования будут служить для подтверждения того, что графические образы плохого качества не были результатом неисправности системы. В случае какого-либо ухудшения качества получаемых графических образов необходимо провести соответствующее корректирующее техническое обслуживание.

5.14 Безопасность и защита

5.14.1 Процедуры обеспечения безопасности

Следует внедрять применимые к организации и целевой задаче указания по безопасности. Такие указания могут, например, иметься в политике и практике компании, отраслевых руководствах (например, для финансовой отрасли или здравоохранения), национальных и международных стандартах или в виде законодательно-нормативных требований.

В отсутствие внутренних руководств всесторонние указания по безопасности, разработанные с целью удовлетворения потребностей организации, можно найти в имеющихся публикациях. Эти указания по безопасности могут послужить адекватной основой для разработки руководств, соответствующих требованиям организации. Некоторые организации могут рассмотреть возможность использования внешних аккредитованных схем обеспечения безопасности в качестве дополнительного подтверждения соответствия своей политике в области безопасности.

Процедуры, реализованные в соответствии с политикой информационной безопасности организации, должны быть задокументированы.

Для управления доступом к различным уровням системы (например, средства управления, средства ввода данных и извлечения информации) следует внедрить защищенную систему управления доступом.

Размещение и среда функционирования для доверенной системы управления документами и информацией, а также хранения, маркировки, обработки, перевозки и обслуживания носителей информации должны соответствовать рекомендациям поставщиков и/или соответствующим национальным или международным стандартам.

Центральная часть системы (включая файловые серверы, подсистемы хранения и т. д.) должна быть размещена в защищенных зонах (в соответствии с процедурами обеспечения безопасности в организации) с документированным ограниченным доступом.

5.14.2 Ключи шифрования

Для улучшения безопасности и целостности хранимых данных могут быть использованы технологии шифрования. Электронный файл может быть зашифрован целиком, чтобы содержащаяся в нем информация не могла быть извлечена без использования ключа шифрования. Тема шифрования сложна и подвержена постоянным изменениям. За подробными сведениями пользователям настоящего стандарта следует обращаться к авторитетным публикациям по этому вопросу.

При длительном хранении использование шифрования может создать проблемы, особенно если ключи и/или сертификаты по каким-либо причинам окажутся недоступными.

В случае применения шифрования должно обеспечиваться защищенное хранение ключей и их доступность только лицам, авторизованным в качестве ответственных за выполнение действий, требующих доступа к ключам.

Следует внедрять процедуры выдачи и управления ключами шифрования и управления сертификатами.

В случае применения шифрования, а также если существует возможность получения дополнительных преимуществ за счет использования услуг третьей стороны по управлению ключами и их восстановлению или по их ответственному депозитарному хранению (escrow), следует рассмотреть возможность использования таких услуг.

Лицо, первоначально отвечавшее за защищенное управление ключами и сертификатами в организации, может перестать работать в организации, поэтому требуются процедуры, обеспечивающие постоянную доступность ключей и сертификатов.

5.15 Использование услуг, оказываемых по контракту

5.15.1 Общие положения

Специализированные поставщики услуг часто привлекаются к проведению сканирования бумажных документов, индексирования, преобразования и хранения данных и для оказания других услуг. В этом случае:

a) С поставщиком услуг должен быть согласован контракт, детализирующий оказываемые услуги.

b) Если контракт не требует, чтобы подрядчик выполнял все соответствующие требования настоящего стандарта, то процедуры инспектирования организацией оказываемых услуг должны быть такими, чтобы не оставалось сомнений относительно полноты, качества и точности этих услуг.

Процедуры и рекомендации, приведенные в настоящем пункте, охватывают услуги любого вида, в том числе предоставляемые на основе административно-хозяйственного управления оборудованием и сооружениями (facilitiesmanagement) и обеспечивающие:

- применение при выполнении работы поставщиками услуг таких же процедур подтверждения аутентичности получаемой информации, как и в том случае, если бы работа целиком выполнялась в организации-клиенте;

- возможность организации-клиента через много лет после события доказать исполнение установленных требований, даже если поставщик услуг прекратил к тому времени свою деловую деятельность.

Если работа выполняется за пределами организации, то следует задокументировать сведения о процедурах, применяемых при передаче информации и/или ее носителей от клиента к поставщику услуг, а также от поставщика услуг — клиенту.

Если поставщик услуг применяет процедуры, соответствующие политике, то клиент должен получать копии либо иметь при необходимости доступ к документации поставщика услуг по вопросам обеспечения соответствия.

5.15.2 Процедурные вопросы

В идеальных условиях, когда поставщик услуг способен доказать реализацию им процедур, соответствующих политике в области управления документами информацией, контракт должен лишь под-

тверждать такую ситуацию и включать в себя согласованные процедуры для проверки соответствия установленным требованиям.

Если поставщик услуг будет действовать в соответствии с согласованными процедурами, то контракт должен включать в себя положения, подробно описывающие, в какой степени эти процедуры будут внедряться и подвергаться аудиту.

Ниже перечислены процедуры и процессы, которые необходимо принять во внимание и включить, по мере необходимости, в контракт:

- клиент должен убедиться в том, что поставщик услуг способен выдавать результаты, соответствующие согласованным требованиям к качеству;

- клиент должен убедиться в том, что поставщик услуг способен обработать выборку из исходного материала и выдать результаты на предложенном носителе информации и в предложенном формате, которые могут быть успешно загружены в целевую систему клиента. Эту выборку следует сохранить;

- клиент должен убедиться в том, что поставщик услуг способен предоставить копию контрольной информации по выполненной обработке в читаемом виде;

- если предоставляются услуги по индексированию, то клиент должен выяснить у поставщика услуг, являются ли предлагаемые требования к точности индексирующих данных приемлемыми и документированными;

- клиент должен убедиться в том, что предлагаемое место выполнения работ является приемлемым и отвечает критериям безопасности, соответствующим потребностям клиента;

- клиент должен убедиться в том, что предлагаемые процедуры и процессы влекут не больший риск причинения ущерба материалу клиента, чем собственные процедуры клиента;

- в случае, если обрабатываемый материал является уникальным или особо ценным, клиент должен убедиться в том, что в предлагаемом месте выполнения работ установлены эффективные системы обнаружения и предотвращения пожара;

- если важное значение имеет безопасность обрабатываемого материала, то клиент должен убедиться в том, что поставщик услуг готов поручиться за надежность персонала, намеченного для выполнения работ. Плюсом является подписание всеми сотрудниками организации — поставщика услуг в качестве одного из условий приема на работу соглашения о конфиденциальности;

- если бумажные документы отправляются на сканирование, то поставщик услуг и клиент должны принять меры, направленные на то, чтобы эти документы оставались доступными клиенту в то время, когда они находятся вне территории клиента.

5.15.3 Транспортировка бумажных документов

Если бумажные документы физически перемещаются от клиента на территорию поставщика услуг, то возникают возможности для их утраты или повреждения. Процедуры должны быть согласованы, с тем чтобы обеспечить приемлемость уровня этого риска. Каждая партия материала, отправляемая или получаемая клиентом и поставщиком услуг, должна сопровождаться контрольным документом, идентифицирующим объекты и указывающим их число.

Все транспортируемые материалы должны быть надлежащим образом упакованы во избежание риска повреждения при транспортировке.

Получателю следует тщательно проверить полученные материалы по товарно-транспортному документу и сообщить отправителю о несоответствиях настолько скоро, насколько это практически возможно.

Транспортные услуги могут оказываться собственной организацией пользователя, третьей стороной или независимым перевозчиком.

В качестве третьей стороны, оказывающей транспортные услуги, следует выбирать организации, доказуемо соответствующие критериям клиента в отношении качества и надежности.

Следует фиксировать дату и время передачи материала транспортной службе, а также дату и время его получения поставщиком услуг; соответствующий документ должен быть подписан лицами, передавшими и получившими материал. Так же следует поступать при получении возвращаемого материала.

5.15.4 Использование услуг доверенной третьей стороны

Надежным способом выявления любых манипуляций с файлом данных, а также проверки его содержимого является сохранение копии файла у доверенной третьей стороны.

В случае использования такого способа следует подготовить заверенную копию электронного файла и доставить ее физически (на носителях) или электронно доверенной третьей стороне с использованием защищенных средств доставки.

Доверенная третья сторона должна выполнять соответствующие процедуры хранения информации, рекомендованные в настоящем стандарте, и быть готова и способна продемонстрировать так же, как и владелец информации, эффективность и безопасность своих услуг.

Примечание — Требования безопасности к доверенным третьим сторонам часто являются более строгими, чем используемые в самих организациях, чью информацию доверенные третьи стороны хранят.

В случае использования для аутентификации цифровых подписей организация вместо сохранения цифровых подписей в собственной системе может передать цифровые подписи файла доверенной третьей стороне. Третья сторона обеспечивает защищенное хранение цифровых подписей, с тем чтобы впоследствии их можно было получить.

5.16 Автоматизация деловых операций (workflow)

Некоторые системы управления документами и информацией имеют функциональные возможности для автоматизации деловых операций (workflow). Такие системы обеспечивают процедурную автоматизацию деловых процессов путем управления последовательностью рабочих операций и активизации соответствующих людских и системных ресурсов, связанных с шагом операции.

В случае использования workflow-систем автоматизации деловых операций сведения об их функционировании (например, диаграммы последовательности операций), классификации описаний и описания workflow-процессов следует задокументировать.

Жизненные циклы workflow-процессов (process definition lifecycles) включают в себя следующие этапы:

- описание (definition);
- разработка;
- реализация;
- прекращение использования;
- модификация.

Все хранящиеся в workflow-системе данные (базы данных, контрольная информация и т. д.) следует проанализировать на предмет наличия требований к срокам их хранения и, там где это применимо, хранить их в соответствии с политикой управления документами и информацией.

В случае внесения изменений в workflow-систему следует использовать процедуры управления изменениями с целью обеспечения того, чтобы сохраненная информация не терялась при выполнении этой процедуры.

Если реализуются специализированные (ad hoc) workflow-процессы (т. е. такие, правила которых могут быть изменены или созданы по ходу работы процесса), то следует сохранить полную контрольную информацию о процессе вместе со сведениями, идентифицирующими персонал, который внес изменения в стандартные workflow-процедуры.

5.17 Отметки даты и времени

Процедуры регулярной проверки системных часов на точность выдаваемых ими даты и времени должны быть задокументированы. Все ошибки должны быть исправлены и все предпринятые действия задокументированы.

Если часы переустанавливают в зависимости от времени года, например, переводят на летнее время, то выполняемые при этом процедуры должны быть задокументированы.

Только авторизованный персонал должен иметь возможность изменять показания системных часов.

Если существует особая необходимость продемонстрировать точность отметок даты и времени, то следует рассмотреть возможность использования услуг доверенной третьей стороны. Если используется доверенное время, то процедуры, демонстрирующие целостность и аутентичность отметки времени и ее связь с конкретным информационным объектом, должны быть задокументированы.

5.18 Контроль версий

5.18.1 Информация

В некоторых приложениях электронные информационные материалы (documents) могут подвергаться изменениям. Типичным примером являются приложения, применяемые для управления техническими чертежами в конструкторских бюро. Со временем могут быть созданы несколько различных версий электронного информационного материала, при этом каждому из них назначается номер версии. В таких приложениях важно сохранять каждую версию как отдельный электронный информационный материал, а также поддерживать взаимосвязи между версиями.

В случае, если допускается внесение изменений в хранящиеся электронные объекты, процедуры авторизации и осуществления таких изменений должны быть задокументированы.

Должна быть доступна документация, касающаяся всех требований к сохранению предыдущих версий таких файлов.

5.18.2 Документация

Для обеспечения того, чтобы для любого документа, относящегося к соблюдению установленных требований, можно было идентифицировать его версию, соответствующую заданному моменту времени в пределах его жизненного цикла, может быть внедрена система контроля версий. Желательно, чтобы процедура контроля версий охватывала всю документацию.

Замененные версии должны сохраняться, как минимум, в течение того же периода времени, в течение которого хранится соответствующая информация[1)].

Этот процесс ведения документации требуется документировать, с тем чтобы можно было описать и засвидетельствовать политики и процедуры, действовавшие на момент ввода информации в систему и в последующее время. Если этого не сделать, то возникнет риск успешной компрометации целостности информации. Если, например, нет уверенности в том, какие именно процедуры сканирования использовались для создания и ввода несколько лет тому назад графического образа бумажного документа и какие процедуры хранения соблюдались в последующее время, то может быть сложно или невозможно опровергнуть сомнения в аутентичности и целостности этой информации.

5.18.3 Процессы и процедуры

Все изменения в процедурах и/или процессах должны осуществляться в соответствии с утвержденной процедурой контроля изменений.

5.19 Поддержание документации в актуальном состоянии (maintenance of documentation)

Для соответствия политике управления документами и информацией требуется наличие и использование указанной документации. Процедуры поддержания этой документации в актуальном состоянии должны быть включены в руководство по процедурам. Процедуры поддержания документации в актуальном состоянии должны включать в себя документирование этой деятельности.

Поддержание документации в актуальном состоянии необходимо в связи с тем, что с течением времени требования будут эволюционировать, а законодательство и технологии — меняться. В некоторых случаях будет достаточно разовых усилий по актуализации, осуществляемых в качестве реакции на замеченные изменения. Кроме того, как правило, в отношении более важной информации, уместны регулярный плановый анализ и пересмотр.

Процедуры, обеспечивающие поддержание документации в актуальном состоянии, должны быть задокументированы.

В отношении этой документации должны соблюдаться правила управления документами, которые, как минимум, должны быть не хуже тех, что применяются в отношении других важнейших деловых документов организации.

В частности, в случае пересмотра какого-либо из элементов документации, копия его состояния до внесения изменений должна сохраняться в течение, как минимум, того же периода времени, что и информация, к которой он относится.

Хранение этой документации должно быть организовано так, чтобы соответствующие авторизованные стороны (например, аудиторы) могли идентифицировать и извлечь всю документацию, действовавшую на любой заданный момент времени.

Документация может храниться в электронном виде в доверенной системе управления документами и информацией с применением тех же мер контроля и управления, которые предусмотрены настоящим стандартом, либо в бумажном виде или на микроформах в защищенных местах хранения, либо с использованием любой комбинации этих методов.

Политика, принятая в отношении хранения документации по обеспечению соответствия установленным требованиям, должна быть отражена в политике.

В большинстве случаев было бы желательно, чтобы изменения документировались так, чтобы у заинтересованной стороны была возможность отслеживать изменения между версиями. Этого можно добиться путем документирования истории изменений для каждой части документации.

[1)] В случае необходимости в суд или контролирующий орган могут быть представлены действовавшие в соответствующий период времени версии внутренних нормативных документов.

6 Ключевые технологические вопросы (enabling technologies)

6.1 Общие положения

В настоящем разделе рассматриваются связанные с технологией вопросы, имеющие значение для настоящего стандарта, в том числе:

- руководство по системе (см. 6.2);
- выбор носителей информации и подсистемы хранения (см. 6.3);
- уровни доступа (см. 6.4);
- контроль целостности системы (см. 6.5);
- обработка графических образов (см. 6.6);
- методы сжатия (см. 6.7);
- разделение формы и введенной информации, «снятие» формы (см. 6.8);
- факторы окружающей среды (см. 6.9);
- миграция (см. 6.10);
- удаление и/или уничтожение информации (см. 6.11).

6.2 Руководство по системе (system description manual)

В руководство по системе следует включать описания составляющих систему оборудования, программного обеспечения и сетевых элементов, а также их взаимодействия.

Должны быть задокументированы подробные сведения о конфигурациях системы.

Подробная информация обо всех изменениях в системе должна быть задокументирована. Такая документация должна включать в себя подробные сведения обо всех процессах, выполненных при внесении изменений.

Руководство по системе должно быть структурировано так, чтобы можно было легко получить подробные сведения о системе на любой момент времени в течение периода ее эксплуатации, что могло бы достигаться путем создания новой версии руководства каждый раз, когда в систему вносятся изменения, с тем чтобы можно было получить доступ к четкому описанию системы по состоянию на определенный момент времени в прошлом.

Для уже функционирующих систем информация, сохраненная в системе до достижения соответствии с политикой управления документами и информацией, не может рассматриваться как отвечающая положениям политики, за исключением случаев, когда меры контроля и процедуры, описанные в политике, были реализованы в системе с момента сохранения этой информации.

Пользователь должен оценить, соответствуют ли элементы системы требованиям соответствующих национальных и/или международных стандартов. Такая оценка дает возможность аудиторам системы проверять эксплуатационные показатели и надежность системы на соответствие этим стандартам.

6.3 Выбор носителей информации и подсистемы хранения (storage media and sub-system considerations)

Риск неумышленного или злонамеренного внесения изменений в сохраненные электронные объекты варьируется в зависимости от типов подсистемы хранения и носителей информации. Также варьируется способность обнаруживать все такие изменения. Например, при использовании носителей информации однократной записи, как правило, невозможно модифицировать однажды сохраненные электронные файлы, поскольку следствием любой такой модификации станет разрушение по крайней мере части данных, что приведет к порче, если не к полной нечитаемости файлов. И наоборот, при применении систем, использующих он-лайн хранение информации, никогда нельзя полностью гарантировать отсутствие несанкционированных изменений (обычно обеспечиваемое средствами управления доступом).

Электронные объекты, хранящиеся на магнитных дисках и других перезаписываемых носителях информации прямого доступа, могут, в принципе, быть изменены. При использовании таких носителей риск несанкционированных изменений связан не столько с самим носителем, сколько с мерами контроля, реализованными подсистемой хранения и программным обеспечением, которое управляет доступом. Для того чтобы модифицировать файлы, нужен доступ на чтение и запись, и хорошо спроектированные системы снабжены средствами контроля для предотвращения несанкционированного получения такого доступа. Пользователи, имеющие доступ только на чтение, не могут модифицировать файлы. Одного этого, однако, недостаточно, если система не ведет защищенный протокол всех случаев доступа на чтение и запись. Дополнительные накладные расходы на документирование модификаций в системе, в которой файлы модифицируются очень часто, могут быть существенными, однако без такого документирования может оказаться невозможным обнаружение несанкционированных

изменений, сделанных квалифицированным хакером или кем-то из тех, кто имеет соответствующие права доступа.

В случае перезаписываемых носителей последовательного доступа (таких, например, как магнитные ленты) внести несанкционированные изменения сложнее, чем в случае носителей информации прямого доступа, поскольку если модифицируемый файл не был записан на конкретном носителе последним, то придется скопировать и перезаписать также и все последующие файлы. Несанкционированные действия с носителем может быть легче осуществить после его отключения/снятия, если злоумышленнику удалось получить к нему доступ. Поэтому важной является задача обеспечения физической безопасности неподключенных носителей и управление доступом к носителю, когда он подключен (он-лайн).

Следует документировать прохождение этапа прикладных процессов, на котором программное обеспечение запрашивает запись электронных файлов в систему хранения.

Носители информации и взаимосвязанные подсистемы хранения должны выбираться так, чтобы предотвратить возможность недетектируемого внесения несанкционированных дополнений, изменений и/или удаления информации. Процедуры детектирования могут включать в себя использование электронных/цифровых подписей и/или копий, сохраняемых в различных местах, предпочтительно с привлечением доверенных третьих сторон.

В системах, не оборудованных средствами, позволяющими в ходе нормальных операций автоматически обнаруживать несанкционированные изменения или удаления файлов, пользователям следует проводить выборочные проверки, с тем чтобы убедиться в том, что не подлежащие модификации (frozen) файлы не были изменены или удалены.

В случае использования носителей однократной записи следует принять во внимание сроки хранения сохраняемой информации. Там, где это практически возможно, информацию с различными сроками хранения не следует сохранять в одном физическом разделе носителя информации.

6.4 Уровни доступа

Подробные сведения обо всех имеющихся в системе уровнях доступа и о процедурах их использования должны быть задокументированы.

Обычно имеются следующие уровни доступа:

- руководитель системы (system manager);
- системный администратор;
- сотрудник службы технической поддержки системы (system maintenance);
- авторы и отправители (originators);
- хранение и индексирование информации;
- поиск информации.

Следует разрешать ввод или изменение хранимой информации только сотрудникам, имеющим соответствующие права доступа.

Права доступа к системе должны предоставляться только после того, как сотрудник успешно подтвердил свою компетентность.

6.5 Контроль целостности системы (system integrity checks)

6.5.1 Общие положения

Внутри системы должны иметься средства, обеспечивающие в масштабах всей системы поддержание целостности сохраненной информации, в том числе во время ее передачи с носителей/на носители информации.

Приемлемым подходом является использование контрольных сумм, вычисленных сразу же после ввода информации в систему. Использование данного метода гарантирует, что любые ошибки при передаче файлов между подсистемами будут обнаружены автоматически и со всей определенностью. Сам по себе этот метод не защищает от возможности злонамеренного манипулирования информацией между моментом ввода информации в систему и временем перенесения ее на носитель информации. Такие манипуляции могут сопровождаться вычислением новой контрольной суммы, если алгоритм вычисления контрольных сумм известен. Для решения этой проблемы требуются иные процедуры. Простым способом является сохранение каждой вычисленной контрольной суммы в составе контрольной информации (audit trail).

Для защиты хранимой информации от вредоносного программного обеспечения следует установить и поддерживать в актуальном состоянии соответствующее защищающее программное обеспечение.

Следует установить там, где это уместно, оборудование для защиты системы от сбоев питания.

6.5.2 Цифровые и электронные подписи (включая биометрические подписи)

Цифровые и электронные подписи дают возможность показать, что извлеченная информация является именно той информацией, которая была сохранена. Для внедрения таких систем подписания обычно требуется сотрудничество обеих сторон. Подписи создаются с помощью устройств оцифровки подписи (электронные подписи) либо с помощью ключа (цифровые подписи) и ассоциируются с электронным файлом. В ряде случаев лицо, извлекающее информацию, может использовать подпись для проверки личности первоначального подписанта, а также — в некоторых системах подписания — для проверки целостности файла. Данные методы могут быть использованы при хранении, выполнении workflow-процессов и передаче (независимо от того, используются ли системы передачи в реальном времени или системы отложенной передачи). Подписи следует использовать в тех приложениях, где важно иметь возможность подтвердить целостность полученного файла и, возможно, личность отправителя. Следует обеспечить защищенное хранение подписей. Доступ к файлам подписей, ключам и алгоритмам должен разрешаться только авторизованному персоналу.

Цифровые и электронные подписи, используемые для доказательства неизменности электронной информации, должны включать в себя контрольные суммы или значения хешей, которые могут быть встроены в файлы и/или сохранятся в защищенной системе с привязкой к исходной информации.

Процессы, используемые для выдачи, поддержания и/или создания цифровых и электронных подписей, должны быть задокументированы. Эти процессы должны включать в себя механизмы проверки истинной личности лица до того, как ему будут предоставлены права подписания.

В случае возникновения сомнений относительно аутентичности электронных файлов подписи могут быть использованы в качестве доказательства, подтверждая, что всякий сохраненный или полученный путем передачи файл содержит ту же информацию, что и исходный файл. Процессы, которые необходимо выполнить в случае, если возникнет вопрос об аутентичности файла, снабженного цифровой подписью, следует задокументировать.

6.6 Обработка графических образов

Для получения графических образов оптимального качества или для повышения качества распознавания в процессе автоматизированного ввода данных могут быть выполнены процессы обработки после сканирования. Если такие процессы выполняются, то воздействие каждого из этих процессов на графический образ должно быть задокументировано индивидуально.

Термин «процессы, выполняемые после сканирования» используется для описания различных методов улучшения качества изображения, использующих аппаратные и/или программные средства, которые могут повлиять на отображение графических образов и размер сохраняемых файлов. Такие средства могут быть установлены как на рабочей станции сканирования, так и на сетевом сервере.

В число наиболее распространенных методов обработки входят:

- выравнивание перекосов (de-skew);
- удаление точек и пятен, очистка фона (de-speckle/backgroundclean-up);
- удаление черной каймы по границе изображения;
- «снятие» формы (см. также 6.8).

Средства обработки графических образов следует использовать с осторожностью. Например, процесс удаления точек и пятен может удалить десятичные точки, тем самым изменив значение чисел.

Любая обработка оцифрованного графического образа не должна повлиять на его целостность как истинной копии оригинала. Чтобы убедиться в том, что обработка не влияет на целостность отсканированных графических образов, следует отсканировать тестовый набор бумажных документов, включив в него обработку изображений, и сопоставить распечатки полученных графических образов с оригиналами.

В случае, если применяются методы обработки графических образов, следует подумать о сохранении графических образов тестового набора бумажных документов, полученных как с использованием обработки, так и без нее.

Эффект от обработки полутонового графического образа перед его преобразованием в черно-белое изображение следует проверять на приемлемость.

Средства удаления точек и пятен следует применять с особой осторожностью и их использование документировать. Использование этих средств приводит к удалению отдельных пикселей или небольших групп пикселей из электронного графического образа, в результате чего получается субъективно более чистое изображение, однако никогда не бывает полной уверенности в том, что из графического образа удален только шум. При обработке определенных видов бумажных документов существует высокий риск того, что может быть удалена полезная информация, например, отдельные части уже искаженных символов, знаки препинания или часть мелких деталей в чертежах.

Если для графических образов обычно проводится удаление точек и пятен, тогда в отсутствие явной информации о конкретных графических образах, подвергшихся такой обработке, впоследствии предполагают, что удаление точек и пятен проводилось для всех изображений, что может негативно сказаться на возможности доказать аутентичность этих графических образов в случае возникновения сомнений в их полноте.

Применение средств удаления точек и пятен должно документироваться в журнале оператора (operator log) либо в составе контрольной информации, либо путем использования дополнительных данных (метаданных), ассоциированных с соответствующим графическим образом.

Если важно, чтобы не было никаких потерь информации в отсканированных графических образах, за исключением потерь, связанных с разрешением при сканировании, то первоначально созданный графический образ не следует впоследствии подвергать какой-либо обработке.

В тех случаях, когда методы обработки графических образов могут повлиять на целостность сохраненного графического образа, следует рассмотреть возможность сохранения также и первоначального (т.е. необработанного) графического образа.

6.7 Методы сжатия

Методы сжатия файлов следует применять в соответствии с политикой управления документами и информацией. Такие методы могут применяться к электронным файлам до или во время хранения, с тем чтобы уменьшить размер файлов и улучшить производительность системы.

Используемый тип сжатия, как правило, зависит от целевой задачи, хотя в некоторых системах может использоваться встроенный механизм сжатия, и тогда у пользователя нет иной альтернативы, кроме его применения. Дополнительные сведения о методах сжатия можно найти в ИСО/ТО 12033.

Методы сжатия могут основываться на различных математических подходах, однако все они могут быть разделены на два класса: сжатие с потерями и сжатие без потерь.

Применяемые методы сжатия и наличие либо отсутствие потерь при их использовании должны быть задокументированы. Документация должна содержать количественные данные и включать в себя описание алгоритма, использованного для расчета уровня потерь при сжатии.

Эта информация может сохраняться как часть файла или взаимосвязанных с ним данных либо в отдельном журнале.

Примечание — Например, в случае графических файлов в формате TIFF (и в некоторых других форматах) сведения о методе сжатия автоматически сохраняются внутри графического файла.

Методы сжатия с потерями следует использовать с осторожностью. По определению применение таких методов приводит к необратимой потере данных, пусть даже в некоторых случаях это потеря является неощутимой визуально. Как следствие, распакованный электронный файл не будет идентичен первоначальному файлу, что может затруднить доказательство целостности таких файлов. Например, в графическом файле часть текста и/или рисунков может пропасть, будучи замененной искусственно сгенерированными данными. Таким образом, возможен риск при использовании сжатия с потерями в отношении файлов, в первую очередь, содержащих текст (в том числе рукописный), чертежи и штриховые рисунки (line drawings).

Сжатие с потерями может быть пригодно для фотографических и иных материалов с непрерывным изменением оттенков; для полутоновых и цветных документов, если можно показать, что в отсканированных графических образах отсутствует существенная потеря информации.

Если применяется сжатие с потерями, то следует сопоставить тестовый набор распакованных файлов с их оригиналами, с тем чтобы убедиться в отсутствии существенной потери информации.

Если применяются методы сжатия с потерями, то следует задокументировать достигнутые степени сжатия.

Степень сжатия следует по возможности выбирать такой, чтобы вся информация, необходимая в контексте целевой задачи, присутствовала в распакованном файле.

Максимально допустимая степень сжатия может быть определена с использованием тестовой выборки исходных документов и может варьироваться для различных документов выборки. Возможно, потребуется принять решение о том, использовать ли различные степени сжатия для различных документов или использовать одну и ту же степень сжатия для всех документов. В случае использования последнего подхода результатом, как правило, будет больший средний размер графического файла, однако скорость обработки также будет выше из-за меньшего вмешательства оператора.

Если важно, чтобы не было потерь информации в отсканированных графических образах, за исключением потерь, связанных с разрешением при сканировании, то сжатие с потерями использовать не следует. К числу электронных документов, для которых использование методов сжатия с потерями не

рекомендуется, относят, например, рентгенограммы (т. е. медицинские и инженерные рентгеновские снимки).

В случае применения сжатия система должна включать в себя адекватные, предпочтительно автоматизированные средства, обеспечивающие соответствие сжатых файлов требованиям к контролю качества (таким, например, как проверка качества графического образа после сканирования с возможностью проведения при необходимости повторного сканирования; контроль над точностью ассоциированных данных; контроль целостности данных).

6.8 Разделение формы и введенной информации, «снятие» формы (form overlays and form removal)

Если исходный документ представляет собой форму, на которую наложена информация, то форма может быть электронным образом удалена из отсканированного графического образа перед его сохранением («снятие» формы).

Если электронным образом снятая форма сохраняется отдельно от отсканированных графических образов, к которым она относится, ею следует управлять так, как если бы она была частью отсканированного графического образа.

Следует задокументировать тот факт, что полученный графический образ (без формы) является результатом снятия формы, а также идентификатора всех шаблонов, использованных при снятии формы. Эта информация должна сохраняться в привязке к полученному графическому образу. Также должны быть сохранены копии всех использованных шаблонов.

Копия, полученная путем слияния шаблона и графического образа со снятой формой, может не признаваться точной копией оригинала, хотя она может быть достаточно точной для использования в приложениях.

Аутентичность такого синтезированного графического образа может быть трудно доказать, особенно если на синтезированном изображении имеет место очевидное смещение информации относительно формы.

Может оказаться целесообразным сохранять точные копии первоначальных форм, сохраняя сами оригиналы либо изготавливая их копию на микропленке, либо сохраняя полные графические образы форм.

6.9 Факторы окружающей среды (environmental considerations)

Следует задокументировать описание рекомендаций производителей относительно условий функционирования всех компонентов системы и носителей информации.

Также следует задокументировать процедуры обращения с носителями информации и их хранения.

Все виды носителей информации имеют ограниченный срок службы. Для обеспечения возможности извлечения сохраненной информации необходимо проводить регулярные проверки носителей информации в соответствии с рекомендациями производителя. Процедуры контроля состояния носителей информации должны быть задокументированы. Носители должны регулярно проверяться в соответствии с рекомендациями их производителя.

6.10 Миграция

Информация может храниться в течение достаточно длительного времени и, что важно, дольше, чем время жизни ныне используемых технологий. Поэтому для обеспечения целостности хранимой информации важно с самого начала предусмотреть возможность того, что она подвергнется процессам миграции. Такие процессы могут включать в себя смену носителя информации и/или изменение компьютерного оборудования и/или программного обеспечения.

Надежным методом решения этой потенциальной проблемы является обеспечение хранения электронных файлов в стандартном для отрасли формате либо для поддержания программ просмотра (viewers) для каждого формата, используемого для хранения информации.

Следует предусмотреть возможность миграции электронных файлов (включая метаданные, индексирующие данные и контрольную информацию) на новые технологии без потери целостности и с достаточной документацией процесса миграции, позволяющей впоследствии в любой момент времени подтвердить целостность сохраненной информации.

6.11 Удаление и/или уничтожение (expungement) информации

Может оказаться необходимым удалить/уничтожить информацию в доверенной системе управления документами и информацией, например, во исполнение законодательно-нормативных требований.

Иногда обстоятельства могут потребовать, чтобы информация, уже отобранная на уничтожение в связи с истечением обычного для нее срока хранения, временно не уничтожалась. Следует реализовать

процессы, обеспечивающие проведение экспертизы уничтожаемой информации перед выполнением уничтожения, с тем чтобы учесть возможность таких особых обстоятельств.

Если информация хранится на носителях однократной записи типа WORM, то удаление какой-то определенной информации невозможно (если только не реализован контролируемый процесс избирательного копирования на новый носитель информации). В некоторых приложениях можно считать, что удаление всех ссылок на информацию в индексе практически равноценно удалению самой информации. В некоторых приложениях может быть достаточно пометить информацию как удаленную. В случае необходимости организация должна убедиться, что реализованная процедура приемлема для соответствующих контролирующих органов. К этим процессам следует относиться с осторожностью, поскольку в определенных обстоятельствах, тем не менее, может быть предъявлено требование извлечь эту «удаленную» информацию.

Если требуется окончательно удалить информацию из системы, то выявление и удаление всех копий информации (включая резервные копии) обеспечивает надлежащее выполнение этой задачи.

Доверенная система управления документами и информацией должна иметь средства для удаления либо невосстановимого уничтожения информации в рамках проверяемого (auditable) процесса.

В случае, если осуществляется удаление и/или невосстановимое уничтожение информации, соответствующая авторизация должна быть получена до выполнения действий.

Доверенная система управления документами и информацией должна иметь средство для исправления неправильной и удаления ненужной информации.

Если исправление или удаление осуществляются в соответствии с законодательно-нормативными требованиями, они должны соответствующим образом документироваться, чтобы иметь возможность подтвердить исполнение требований законодательства.

Дополнительные рекомендации по удалению информации из систем однократной записи см. в ИСО/ТО 12037.

7 Контрольная информация (audit trails)

7.1 Общие положения

7.1.1 Состав контрольной информации (audit trail data)

При подготовке информации для использования в качестве доказательства какого-либо события или транзакции часто бывает необходимо представить дополнительную поддерживающую информацию. Эта информация может включать в себя такие сведения, как дата сохранения информации, данные о перемещении информации с носителя на носитель и доказательства контролируемого функционирования системы. Эти сведения называются «контрольной информацией» (audit trail information). Контрольная информация (в таком виде, в каком она описана в настоящем стандарте) представляет собой совокупность информации, необходимой для документирования истории всех существенных событий, связанных с хранимой информацией и доверенной системой управления документами и информацией. Эти сведения можно подразделить на две категории:

- относящиеся к системе;
- относящиеся к хранимой информации.

В интересах подтверждения целостности и аутентичности хранимой информации следует документировать историю происходящих в доверенной системе управления документами и информацией действий и событий, которые, возможно, в будущем придется реконструировать.

Контрольная информация должна содержать сведения, необходимые и достаточные для доказательства аутентичности хранимой информации.

Доступ к контрольной информации часто может быть нужен нескольким подразделениям и/или сотрудникам организации (либо внешних организаций), включая представителей деловых подразделений, юридической службы и службы аудита.

Состав контрольной информации должен быть согласован со всеми соответствующими подразделениями организации.

В большинстве организаций контрольная информация будет представлять собой набор журналов (logs), ведущихся системой и операторами.

Контрольная информация должна включать в себя данные об изменениях в информации, хранящейся в системе.

7.1.2 Создание контрольной информации

Насколько это практически возможно, контрольная информация должна создаваться системой автоматически, и соответствующие процессы должны быть описаны в руководстве по системе.

В случае, если входящие в состав контрольной информации данные не создаются системой автоматически, процедуры формирования таких данных должны быть задокументированы в руководстве по процедурам. Следует принять во внимание, что именно отражают эти данные. Например, создается ли определенная часть информации в виде проекта, развивается ли она в виде ряда версий? Требуется ли полная контрольная информация по каждой версии или только для окончательного документа?

Автоматическое создание контрольной информации является предпочтительным, поскольку такой контрольной информацией проще управлять и подтверждать ее подлинность. Если автоматическое создание контрольной информации не используется, то следует тщательно оценить ресурсы, необходимые для создания автоматизированного процесса.

Процедуры, которые должны быть выполнены в случае заполнения файла с контрольной информацией заданного максимального размера, а также процедуры, позволяющие выявить данную ситуацию, должны быть задокументированы в руководстве по процедурам.

7.1.3 Дата и время

Каждая запись данных в массив контрольной информации должна включать в себя соответствующие дату и время, относящиеся к дате и времени документируемого события.

Сохраняемые дата и время события должны быть достаточно точны, чтобы при последующем расследовании установить последовательность событий.

В случае создания контрольной информации системой данные должны быть созданы непосредственно после документируемого события.

Дата и время, как правило, будут датой и временем создания контрольной информации, однако если создание этой информации по существу происходит одновременно с документируемым событием, то это время во всех смыслах будет временем самого события.

В случае создания контрольной информации вручную ее следует создавать как можно скорее после документируемого события. Например, если документируется начало работы оператора, то данный факт следует задокументировать в тот же момент времени. Если документируется начало подготовки конкретного пакета бумажных документов, то данный факт следует задокументировать непосредственно перед началом подготовки этого пакета.

Если фактическое время события имеет важное значение, то следует рассмотреть возможность использования доверенного времени (см. 5.17).

7.1.4 Хранение контрольной информации

Хранение контрольной информации — это тема, которая часто не рассматривается в политике управления документами и информацией организации. Поскольку такого рода данные часто создаются автоматически и редко используются, о них забывают и должным образом не контролируют.

Некоторые системы контролируют размер файлов контрольной информации, используя метод циклической перезаписи, при котором устанавливается максимальный размер файла данных и при достижении этого размера новые данные записываются на место самых старых данных в файле. Таким образом, старая контрольная информация теряется.

Контрольная информация должна быть включена в политику в качестве отдельного типа документа.

Контрольная информация должна сохраняться, как минимум, в течение того же периода времени, что и информация, к которой она относится.

7.1.5 Доступ к контрольной информации

Соответствующим операторам в определенные моменты времени требуется доступ к контрольной информации. В некоторых приложениях такой доступ может требоваться лишь в особых случаях, и поэтому важно, чтобы процедуры доступа и интерпретации контрольной информации были задокументированы.

Руководство по процедурам должно описывать, как можно получить доступ к контрольной информации и как ее интерпретировать.

Контрольная информация должна быть доступна для инспекции авторизованным внешним персоналом (например, аудиторами), слабо знакомым или вообще не знакомым с системой.

7.1.6 Безопасность и защита контрольной информации

Если аутентичность хранимой информации ставится под сомнение, то целостность контрольной информации может оказаться ключевым фактором для установления аутентичности хранимой информации. Уровень защищенности хранимой контрольной информации должен быть достаточным для предотвращения любых изменений в любых данных, входящих в состав контрольной информации.

Контрольная информация должна храниться защищенным образом согласно соответствующей политике информационной безопасности. В отношении контрольной информации должны соблюдаться

внутренние правила управления документами, которые, как минимум, должны быть неприменяемы в отношении других важнейших деловых документов организации.

Следует хранить защищенные резервные копии контрольной информации. Это требование относится к контрольной информации, хранящейся как на электронных носителях, так и на бумаге/микропленке.

Контрольная информация, хранящаяся в доверенной системе управления документами и информацией, должна быть защищена от модификации. В случае использования процедур восстановления файлов следует сохранить контрольную информацию в объеме, достаточном для подтверждения того, что восстановление не повлияло на аутентичность информации.

Для минимизации риска рекомендуется хранить контрольную информацию на WORM-носителях однократной записи. В случае использования перезаписываемых носителей информации необходимо применять дополнительные процедуры для предотвращения внесения изменений. Использование магнитной ленты делает модификацию данных сравнительно затруднительной, поскольку магнитная лента обычно является носителем, запись на который осуществляется последовательно.

Если существует вероятность того, что контрольная информация могла быть модифицирована, то будет сложнее установить аутентичность любой информации, к которой относится эта контрольная информация.

Содержащие контрольную информацию бумажные документы следует чаще убирать с места использования и хранить в защищенном месте. Чем дольше содержащий контрольную информацию документ (например, журнал оператора) остается в относительно небезопасном месте, например, на рабочей станции, тем выше риск внесения в него несанкционированных изменений. В случае документирования контрольной информации на бумажных носителях пользователям необходимо оценить такой риск. При использовании бумажных документов рекомендуется сохранять их копии в доверенной системе управления документами и информацией.

О защите в течение длительного времени с использованием миграции или других методов см. также 7.2.3.

7.2 Контрольная информация по системе

7.2.1 Общие положения

Такие записи данных в составе контрольной информации включают в себя:

- сведения о событии;
- сведения о миграции и конверсии.

7.2.2 Сведения о событии

Для всех данных в составе контрольной информации должна быть возможность установить соответствующий процесс, а также дату и время события.

В зависимости от значения времени и даты информация о них может сохраняться для пакетов (где это уместно) либо для отдельных событий. Если контрольная информация вводится оператором вручную, то может быть непрактично и не нужно создавать контрольную информацию для каждого документа. Например, при подготовке бумажных документов к сканированию может быть достаточно задокументировать время начала и конца обработки пакета; может оказаться достаточным также просто задокументировать, когда оператор начал и закончил работу, при условии, что впоследствии будет возможно установить, какой оператор проводил подготовку и каких именно документов.

7.2.3 Сведения о миграции и конверсии

В случае перемещения информации с одного устройства хранения на другое в качестве части процесса миграции сведения о перемещении должны быть сохранены в составе контрольной информации.

Процедуры миграции и конверсии должны предусматривать методы, посредством которых может быть показано, что все взаимосвязанные данные (такие как метаданные) также подверглись миграции или конверсии.

При использовании иерархических систем хранения (hierarchical storage management systems, HSM), в которых данные постоянно и автоматически без вмешательства пользователя перемещаются между устройствами хранения, создание контрольной информации по этим перемещениям может оказаться ненужно. Возможно, однако, потребуется показать, что система хранения работала нормально в момент передачи информации.

В случае конверсии информации из одного файлового формата в другой сведения о конверсии должны быть сохранены в составе контрольной информации. Например, электронный документ, созданный текстовым процессором, может быть преобразован в графический формат без изменения текста документа. С одной стороны, это не слишком сильно отличается от копирования файла, однако если форматирование имеет значение для информационного контента, то существует вероятность того, что информационный контент преобразованного файла можно будет считать изменившимся.

7.3 Контрольная информация, относящаяся к сохраняемой информации

7.3.1 Общие положения

Такие записи данных в составе контрольной информации включают в себя сведения:

- о процессе сбора и ввода (захвата) информации;
- о пакетах;
- об индексировании;
- о контроле изменений;
- об использовании цифровых подписей;
- об уничтожении информации;
- об управлении workflow-процессами.

7.3.2 Процесс сбора и ввода (захвата) информации

7.3.2.1 Общие положения

Контрольная информация о процессе захвата содержит бесценные сведения, помогающие в установлении аутентичности хранимой информации. Такие сведения, как время ввода, оператор, устройство захвата и тип исходного документа, могут иметь ключевое значение в случае, если аутентичность будет поставлена под сомнение.

В составе контрольной информации следует сохранять ключевые сведения, относящиеся к захваченной или импортированной в систему информации. По каждой процедуре обработки следует сохранить достаточный объем относящейся к ней информации.

Сведения, сохраняемые в составе контрольной информации, обычно содержат:

- идентификационные данные документа или файла;
- отметку даты и времени для процесса;
- идентификатор пакета (при пакетном вводе);
- число страниц (при сканировании документов) или записей данных (при вводе данных);
- положительный результат проверки при контроле качества;
- идентификатор каждого проиндексированного документа или файла;
- идентификаторы оператора и рабочей станции;
- сведения об окончательной записи в хранилище.

Выбор конкретных данных для сохранения в составе контрольной информации зависит от целевой задачи и системы.

7.3.2.2 Сведения о файлах

Информация может собираться и вводиться (захватываться) в систему на уровне файлов, особенно в тех случаях, когда электронные файлы импортируются в систему. Если информация вводится на уровне файлов, то в составе контрольной информации следует сохранить следующие сведения:

1) уникальный идентификатор файла;
2) число документов/страниц в файле;
3) размер файла (например, в килобайтах);
4) формат файла;
5) использованная система кодирования (например, значения полей EDI, DTD и т. д.).

7.3.2.3 Сведения об отсканированных документах

Информация может быть введена в систему путем сканирования исходных документов.

Если используется сканирование документов, то в составе контрольной информации нужно сохранить следующие сведения:

1) уникальный внутренний идентификатор документа;
2) число отсканированных графических образов;
3) число страниц, переданных на устройство хранения данных.

7.3.3 Сведения о пакетах

а) Если данные вводятся на уровне пакетов, особенно в приложениях сканирования документов, то в составе контрольной информации нужно сохранить следующие сведения:

1) уникальный идентификатор пакета;
2) идентификатор оператора;
3) тип сканируемого материала, например, бумажные документы, рулоны микропленки, апертурные карты;
4) количество материала в пакете, например, число документов, число страниц (одно/двусторонних), число кадров на микропленке;
5) подробные сведения об обработке графических образов, выполненной в ходе процессов сканирования, если она где-либо отличается от выполняемой по умолчанию обработки графических образов, описанной в руководстве по системе.

b) Контрольная информация должна храниться так, чтобы можно было легко проверить:
   1) что все необходимые действия были выполнены для данного пакета;
   2) сведения обо всех имевших место аномалиях и отклонениях:

Пример — сведения о несовпадении числа страниц, переданных в хранилище, с числом отсканированных страниц;

   3) что были проведены процедуры контроля качества;
   4) что была выполнена требуемая обработка особых ситуаций.

7.3.4 Индексирование

Индексирующая информация играет важнейшую роль в процессе извлечения информации и, таким образом, ее точность имеет ключевое значение для установления аутентичности хранимой информации. Контрольная информация, содержащая детальные сведения о создании и изменении индексов, может быть использована для того, чтобы подтвердить корректное использование процедур индексирования.

В составе контрольной информации необходимо сохранять сведения о дате и времени создания, изменения и удаления каждого из индексных файлов. Контрольная информация должна включать в себя идентификатор каждого проиндексированного документа или файла данных.

Если индексирующие данные изменяются или удаляются, то следует создать соответствующую контрольную информацию. Если в индекс вносятся изменения, то также может быть сохранена подробная информация об изменениях.

Если запись в индексе относится к удаленной или необратимо уничтоженной информации, то этот факт должен быть задокументирован.

7.3.5 Контроль изменений

Если в хранимую информацию вносятся изменения, то должна быть создана и сохранена контрольная информация, идентифицирующая характер изменений, а также сохранено лицо, инициировавшее эти изменения (или программу, если изменение было произведено системой автоматически).

Там, где это уместно, в контрольную информацию следует включить ссылки на предыдущие версии хранимой информации с целью установления характера изменений.

7.3.6 Цифровые подписи

Если применяются цифровые подписи (или иные методы электронного подписания), то в составе контрольной информации следует сохранять следующие сведения:

1) идентифицирующие данные файла;
2) подтверждение личности подписанта (certification of identification), например, сертификат ключа проверки подписи (открытого ключа) подписанта;
3) идентифицирующие данные удостоверяющего органа (authenticating authority);
4) дата и время подписания;
5) квитанция/подтверждение получения;
6) доказательство проверки подписи.

7.3.7 Уничтожение информации

В составе контрольной информации следует сохранять сведения об уничтожении бумажных документов после их сканирования, уничтожении информации по истечении соответствующего срока хранения, а также авторизации уничтожения.

7.3.8 Управление workflow-процессами

Каждый раз, когда определяется новый деловой процесс либо вносятся изменения в существующее определение, это событие следует документировать с целью накопления контрольной информации.

Если используются workflow-системы, то должны быть определены контрольные точки, в которых должна создаваться контрольная информация.

В большинстве workflow-систем контрольные точки имеются на каждом этапе workflow-процесса. Однако для соответствия политике, возможно, не нужно сохранять контрольную информацию со всех таких контрольных точек. Пользователь должен решить, какие контрольные точки важны с точки зрения потенциального значения данных о workflow-процессе в качестве доказательств. Выбранные контрольные точки следует использовать для создания контрольной информации.

Набор выбранных контрольных точек может изменяться по мере изменения workflow-процессов.

Система должна давать возможность авторизованным пользователям выбирать и отменять выбор контрольных точек, в которых создается контрольная информация.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов ссылочным национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 15489-1-2001	IDT	ГОСТ Р ИСО 15489-1—2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»
ИСО 9000—2005	IDT	ГОСТ Р ИСО 9000—2008 «Системы менеджмента качества. Основные положения и словарь»
ИСО/МЭК 27001-2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО 2859-1—1999	IDT	ГОСТ Р ИСО 2859-1—2007 «Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 1. Планы выборочного контроля последовательных партий на основе приемлемого уровня качества»
ИСО/ТО 12033—2009	—	*
ИСО/ТО 12037—1998	—	*
ИСО 12651—1999	—	*
ИСО 12653-2—2000	—	*
ИСО/ТО 18492-2005	—	*

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

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:
IDT — идентичные стандарты.

Библиография

[1] ISO 2859-1[1)] Sampling procedures for inspection by attributes — Part 1: Sampling schemes indexed by acceptance quality limit (AQL) for lot-by-lot inspection

[2] ISO 9000[2)] Quality management systems — Fundamentals and vocabulary

[3] ISO/TR 12033[3)] Document management — Guidance for the selection of document image compression methods

[4] ISO/TR 12037[4)] Electronic imaging — Recommendations for the expungement of information recorded on write-once optical media

[5] ISO 12651[5)] Electronic imaging — Vocabulary

[6] ISO 12653-2[6)] Electronic imaging — Test target for the black-and-white scanning of office documents — Part 2: Method of use

[7] ISO 15489-1[7)] Information and documentation — Records management — Part 1: General

[8] ISO/TR 15489-2[8)] Information and documentation — Records management — Part 2: Guidelines

[9] ISO/TR 18492[9)] Long-term preservation of electronic document-based information).

[10] ISO/IEC 27001[10)] Information technology — Security techniques — Information security management systems — Requirements

[11] The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production[11)] (Принципы конференции Седона: Наилучшая практика, рекомендации и принципы представления электронных документов)

[12] The Sedona Conference Glossaryfor E-Discovery and Digital Information Management[12)] (Конференция Седона: Глоссарий терминов в области поиска и представления электронных документов и информации, и управления электронной информацией)

[1)] Действует ИСО 2859-1:1999. См. также ГОСТ Р ИСО 2859-1—2007 Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Часть 1. Планы выборочного контроля последовательных партий на основе приемлемого уровня качества.

[2)] Действует ИСО 9000:2005. См. также ГОСТ Р ИСО 9000—2008 Системы менеджмента качества. Основные положения и словарь.

[3)] Действует ИСО/ТО 12033—2009.

[4)] Действует ИСО/ТО 12037:1998.

[5)] Действует ИСО 12651:1999.

[6)] Действует ИСО 12653-2:2000.

[7)] Действует ИСО 15489-1:2001. См. также ГОСТ Р ИСО 15489-1—2007 Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования.

[8)] Действует ИСО/ТО 15489-2:2001.

[9)] Действует ИСО/ТО 18492:2005. Действующая редакция: второе издание

[10)] Действует ИСО/МЭК 27001:2005. См. также ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

[11)] Действует второе издание (июнь 2007 г.), gost.e-ecolog.ru PRINCP_2nd_ed_607.pdf.

[12)] Действует второе издание (декабрь 2007 г.), gost.e-ecolog.ru TSCGlossary_12_07.pdf.

УДК 651.9:004:006.354 ОКС 37.080:25.040.40

Ключевые слова: управление документацией, информация в электронном виде, рекомендации по обеспечению достоверности, рекомендации по обеспечению надежности

Редактор *В.Н. Копысов*
Технический редактор *В.Н. Прусакова*
Корректор *Л.Я. Митрофанова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 27.07.2012. Подписано в печать 09.08.2012. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,15. Тираж 121 экз. Зак. 675.

ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
gost.e-ecolog.ru gost.e-ecolog.ru
Набрано во ФГУП «СТАНДАРТИНФОРМ» на ПЭВМ.
Отпечатано в филиале ФГУП «СТАНДАРТИНФОРМ» — тип. «Московский печатник», 105062 Москва, Лялин пер., 6.

gost.e-ecolog.ru