ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 54989— 2012/ ISO/TR 18492:2005

ОБЕСПЕЧЕНИЕ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

ISO/TR 18492:2005
Long-term preservation of electronic document-based information
(IDT)

Издание официальное

Москва
Стандартинформ
2013

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 технического отчета, 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 17 сентября 2012 г. № 325-ст

4 Настоящий стандарт идентичен техническому отчету ИСО/ТО 18492:2005 «Обеспечение долговременной сохранности электронных документов» (ISO/TR 18492:2005 «Long-term preservation of electronic document-based information»).

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 издаваемом информационном указателе «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, 2013

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 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Обозначения и сокращения . . . 2
5 Долговременная сохранность . . . 3
5.1 Общие положения . . . 3
5.2 Цели стратегии обеспечения долговременной сохранности . . . 3
5.2.1 Общие положения . . . 3
5.2.2 Читаемость электронных документов . . . 3
5.2.3 Интерпретируемость электронных документов . . . 4
5.2.4 Идентифицируемость электронных документов . . . 4
5.2.5 Доступность электронных документов . . . 4
5.2.6 Понятность электронных документов . . . 5
5.2.7 Аутентичность электронных документов . . . 5
6 Элементы стратегии долговременной сохранности . . . 6
6.1 Общие положения . . . 6
6.2 Обновление носителей . . . 6
6.2.1 Общие положения . . . 6
6.2.2 Переформатирование электронных документов . . . 7
6.2.3 Копирование электронных документов . . . 8
6.3 Метаданные . . . 9
6.3.1 Общие положения . . . 9
6.3.2 Взаимная совместимость (интероперабельность) метаданных . . . 9
6.4 Миграция электронных документов . . . 9
6.4.1 Общие положения . . . 9
6.4.2 Зависимость от программного обеспечения . . . 10
6.4.3 Обновление программного обеспечения и инсталляция нового программного обеспечения . . . 10
6.4.4 Миграция в стандартные форматы . . . 11
6.4.5 Миграция электронных документов из унаследованных информационных систем . . . 11
7 Разработка стратегии долговременной сохранности . . . 12
7.1 Политика обеспечения долговременной сохранности . . . 12
7.2 Контроль качества . . . 13
7.3 Безопасность . . . 13
7.3.1 Общие положения . . . 13
7.3.2 Управление доступом при помощи программных средств . . . 13
7.3.3 Управление физическим доступом . . . 13
7.3.4 Защита от утраты . . . 13
7.3.5 Политика обеспечения безопасности . . . 14
7.4 Контроль и мониторинг климатических условий . . . 14
Приложение А (справочное) Национальные программы обеспечения сохранности электронных документов и другие публикации . . . 15
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов и документов ссылочным национальным стандартам Российской Федерации . . . 17

Введение

Международная организация по стандартизации ИСО (International Organization for Standardization, ISO) является всемирным объединением национальных органов по стандартизации (организаций — членов ИСО). Подготовка международных стандартов обычно ведется в технических комитетах ИСО. Каждая организация — член ИСО имеет право быть представленной в тех технических комитетах, тематика которых представляет для нее интерес. Вместе с ИСО в этой работе также принимают участие международные правительственные и неправительственные организации. ИСО тесно сотрудничает с Международной электротехнической комиссией (МЭК — International Electrotechnical Commission, IEC) по всем вопросам стандартизации в области электротехники.

Международные стандарты разрабатываются в соответствии с правилами, установленными в части 2 директив ИСО/МЭК.

Основной задачей технических комитетов является подготовка международных стандартов. Одобренные техническими комитетами проекты стандартов рассылаются организациям — членам ИСО на голосование. Для публикации в качестве международного стандарта проект должен быть одобрен не менее чем 75 % организаций — членов ИСО, принявших участие в голосовании.

В исключительных случаях, когда технический комитет собрал материалы, отличающиеся от тех, которые обычно публикуются в качестве международного стандарта (например, отражающие текущее состояние дел по соответствующему вопросу), комитет может большинством голосов своих членов принять решение о публикации технического отчета. По своей природе технический отчет носит чисто информативный характер, и его пересмотр не требуется до тех пор, пока содержащиеся в нем сведения не потеряют свою актуальность и полезность.

Следует иметь в виду, что некоторые элементы данного документа могут объектами патентных прав. ИСО не несет ответственности за установление подлинности таких патентных прав.

Технический отчет ИСО/ТО 18492 был подготовлен подкомитетом SC 3 по общим вопросам технического комитета ИСО ТС 171 «Прикладные системы создания и хранения документов» (Document management applications).

Обеспечение долговременной сохранности аутентичной электронной неструктурированной или слабоструктурированной документированной информации (electronic document-based information, далее по тексту — документов) — проблема, которую приходится решать в различных сферах деятельности, таких как архивное дело, управление информацией и документами, электронная коммерция, электронное государственное управление и разработка технологий. Решение данной проблемы осложняется тем, что организации и отдельные лица, на которых возложена ответственность за обеспечение долговременного доступа к аутентичным электронным документам, используют для достижения этой цели различные стратегии.

Несмотря на явную потребность в решении проблемы обеспечения долговременного доступа к аутентичным электронным документам в настоящее время отсутствуют согласованные международные рекомендации по этому вопросу. Как следствие, применяются различные, порой не совместимые между собой методы, что создает для организаций серьезные проблемы, связанные с доступностью и/или аутентичностью сохраняемых электронных документов.

Признавая универсальную проблему технологического устаревания компьютерного оборудования и программного обеспечения, а также ограниченный срок службы цифровых носителей информации, данный стандарт содержит рекомендации организациям — хранителям информации (storage repositories, далее по тексту — хранители информации) по поддержанию аутентичных электронных документов, сохраняемых для использования в будущем, и по обеспечению доступа к ним.

Цель настоящего стандарта — предложить четкую концепцию для разработки стратегий и хороших практик, применимых к широкому спектру электронных документов государственного и частного секторов для обеспечения их долговременной доступности и аутентичности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ОБЕСПЕЧЕНИЕ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Long-term preservation of electronic document-based information

Дата введения — 2013—05—01

1 Область применения

Настоящий стандарт содержит методические указания и рекомендации по обеспечению долговременной сохранности аутентичных электронных документов и доступа к ним в тех случаях, когда срок их хранения превышает расчетный срок использования технологий (оборудования и программного обеспечения), применяемых для создания и поддержания этих документов.

Настоящий стандарт учитывает роль технологически нейтральных ИТ-стандартов в обеспечении долговременного доступа к информации.

Настоящий стандарт рекомендует к обеспечению долговременной сохранности аутентичных электронных документов и доступа к ним привлекать специалистов ИТ, специалистов по управлению информацией/контентом (document managers), специалистов по управлению документами (records managers) и архивистов.

В настоящем стандарте не рассматриваются процессы создания, «захвата» (ввода) и классификации аутентичных электронных документов.

Настоящий стандарт применим к любым видам информации, созданной информационными системами и сохраненной в качестве свидетельства деловых транзакций и деятельности.

Примечание — Электронные документы представляют собой «деловую память» о повседневной деловой деятельности и событиях, давая организациям возможность впоследствии изучать, анализировать и документировать эти действия и события. Электронные документы являются свидетельствами деловых транзакций, что позволяет организациям использовать их при принятии управленческих решений в настоящее время и в будущем, для удовлетворения потребностей клиентов, для обеспечения соответствия законодательно-нормативным требованиям и для защиты интересов организации в случае судебных споров. Поэтому электронные документы должны сохраняться и должным образом храниться.

2 Нормативные ссылки

Перечисленные ниже стандарты и документы, на которые в тексте имеются ссылки, необходимы при применении данного стандарта. Для ссылок, в которых указана дата, применяется только упомянутая версия документа. Для ссылок без указания даты нужно использовать последнюю версию соответствующего документа (включая имеющиеся поправки):

ИСО 12651:1999 Электронная обработка изображений — Словарь (ISO 12651:1999, Electronic imaging — Vocabulary)

ИСО 15489-1 Информация и документация — Управление документами — Часть 1: Общие принципы (ISO 15489-1, Information and documentation — Records management — Part 1: General)

ИСО/ТО 15489-2 Информация и документация — Управление документами — Часть 2: Руководство (ISO/TR 15489-2, Information and documentation — Records management — Part 2: Guidelines)

ИСО/ТУ 23081-1 Информация и документация — Процессы управления документами — Метаданные документов — Часть 1: Принципы (ISO/TS 23081-1, Information and documentation — Records management processes — Metadata for records — Part 1: Principles)

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины и определения, данные в ИСО 12651, ИСО 15489-1 и ИСО/ТО 15489-2, а также следующие термины с соответствующими определениями:

3.1 **аутентичный электронный документ** (authentic electronic document-based information): Электронный документ, точность, надежность и целостность которого сохраняются с течением времени.

3.2 **неструктурированная или слабоструктурированная документированная информация (документ)** (document-based information): Существенная информация, которую можно обрабатывать как единый объект (например, изображение, текст, электронная таблица, представление базы данных).

Примечание — К неструктурированной информации относятся (перечень не является исчерпывающим): тексты, графические образы, табличные данные (например, электронные таблицы) и любые их комбинации.

3.3 **контент (содержание) документа** (document-based information content): Существенная информация, содержащаяся в документе.

3.4 **контекст документа** (document-based information context): Сведения об обстоятельствах создания, контроля, использования, хранения и управления электронным документом, а также сведения о его взаимосвязях с другими подобными документами.

3.5 **структура документа** (document-based information structure): Логические и физические атрибуты документа.

Примечание — Логические атрибуты устанавливают логический порядок (например, иерархию распознаваемых подразделов), в то время как в число физических атрибутов входят такие элементы, как, например, тип шрифта и интервалы.

3.6 **электронное архивирование, электронная архивация** (electronic archiving): Сохранение электронной информации в обособленном физическом или логическом пространстве, где эта информация защищена от утраты, от внесения изменений и деградации.

Примечание — Защищенная таким образом информация может быть в будущем использована в качестве надежного свидетельства (доказательства).

3.7 **долговременная сохранность** (long-term preservation): Период времени, в течение которого электронные документы поддерживаются в качестве доступного и аутентичного свидетельства (доказательства).

Примечание — В зависимости от нужд и потребностей организации этот период может варьироваться от нескольких лет до нескольких сотен лет. Его продолжительность определяется законодательно-нормативными требованиями и деловыми потребностями. В некоторых организациях, таких как архивы государственных документов, период времени, в течение которого необходимо сохранять электронные документы, обычно исчисляется сотнями лет.

3.8 **метаданные** (metadata): Данные, описывающие содержание (включая ключевые слова, используемые для извлечения документов), структуру и контекст электронного документа, а также управление документом во времени.

3.9 **миграция** (migration): Процесс переноса электронных документов из одной программно-аппаратной среды или с одного носителя информации в другую среду или на другой носитель информации, без изменений либо с минимальными изменениями в структуре и без каких-либо изменений в контенте (содержании) и контексте.

3.10 **хранитель информации** (storage repository): Специализирующаяся на хранении информации организация либо подразделение, на которые возложена ответственность за хранение и поддержание аутентичных электронных документов.

Примечание — Данное определение отличается от «технических» определений понятия «хранилище информации» (storage repository).

3.11 **технологическое устаревание (technological obsolescence):** Вытеснение с рынка признанного технического решения вследствие значительных улучшений и развития технологий.

4 Обозначения и сокращения

ASCII (American Standard Code for Information Interchange) — Американский стандартный код для обмена информацией;

CRC (Cyclical Redundancy Code) — циклический избыточный код;

HTML (Hyper Text Markup Language) — язык разметки гипертекста;

JPEG (Joint Photographic Engineers Group) — Объединенная группа специалистов по компьютерной обработке фотографических изображений;

OCR (Optical Character Recognition) — оптическое распознавание символов;

PDF/A-1 (Portable Document Format — Archive) — вариант для архивного хранения формата переносимого документа;

SHA-1 (Standard Hash Algorithm 1) — стандартный алгоритм вычисления хэш-функции №1;

TIFF (Tagged Image File Format) — тегированный формат файлов изображений;

WORM (Write Once Read Many [times]) — носитель информации однократной записи и многократного считывания;

XML (Extensible Markup Language) — расширяемый язык разметки.

5 Долговременная сохранность

5.1 Общие положения

Распространение компьютерных технологий, поддерживающих создание, использование, хранение и сопровождение информации, все чаще приводит к тому, что организации частного и государственного секторов полагаются на электронные документы как на официальное свидетельство своей деловой деятельности. Как следствие, организации все чаще сталкиваются с проблемой обеспечения долговременной доступности созданных в надежных и заслуживающих доверия информационных системах и сохраненных на электронных носителях аутентичных электронных документов и информации. Эти носители могут быть затронуты процессом технологического устаревания, что, в отсутствие корректирующих мер, сделает документы недоступными. Важность этой проблемы возрастает вследствие того, что организации все чаще ведут свою деятельность и совершают транзакции, не документируя их на бумажных носителях.

Таким образом, необходимо, чтобы организации разработали и применяли на практике тщательно продуманные стратегии обеспечения долговременной сохранности аутентичных электронных документов и доступа к ним. Элементы такой стратегии описаны в 5.2.

5.2 Цели стратегии обеспечения долговременной сохранности

5.2.1 Общие положения

В данном подразделе выделены шесть ключевых факторов, которые хранители информации должны принять во внимание при разработке стратегии долговременной сохранности.

5.2.2 Читаемость электронных документов

Стратегия обеспечения долговременной сохранности направлена на то, чтобы электронные документы в будущем оставались читаемыми. Для достижения этой цели составляющий электронные документы поток битов должен быть доступен на той компьютерной системе или устройстве:

- на которой(ом) он первоначально был создан, или
- на которой(ом) он в настоящее время хранится, или
- которая(ое) в настоящее время используется для доступа к нему, или
- которая(ое) будет использоваться для хранения электронной информации в будущем.

Данные четыре варианта обеспечения возможности обрабатывать информацию (processability) исходят из того, что информация, сохраненная на электронном носителе, может со временем стать нечитаемой. Есть два основных сценария, по которым это может произойти.

В первом случае нечитаемость носителя — следствие воздействия неблагоприятных условий хранения. Все виды носителей, используемых в настоящее время для хранения электронных документов, чувствительны к воздействию неблагоприятной среды хранения, например к перепадам температуры и влажности. Подобные неблагоприятные условия или приводят к повреждению носителя, или ускоряют процесс его «старения». Для обеспечения максимального срока службы различных типов электронных носителей информации требуются разные уровни контролируемой среды хранения. При использовании некоторых технологий записи информации порча данных возможна из-за воздействия магнитных полей, пыли и загрязняющих окружающую среду веществ (магнитные носители), в то время как другие виды носителей (оптические носители) менее подвержены влиянию внешних факторов и реже повреждаются при использовании их вне жестко контролируемой среды хранения. Однако какие бы из технологий записи информации ни использовались, необходимо понимать, что все виды носителей информации могут портиться и/или деградировать вследствие воздействия окружающей среды.

Во втором случае нечитаемость может стать следствием морального устаревания носителей, т. е. когда устройство для хранения информации (например, лента или диск) физически несовместимо с имеющимся компьютерным оборудованием (например, приводом для чтения лент или дисков), и, следовательно, информация не может быть прочитана. Моральное устаревание носителей информации представляется неизбежным, поскольку достижения в технологиях хранения постоянно изменяют способы физического хранения электронных документов (происходят, например, изменения в технологии записи, в интерфейсах оборудования/программного обеспечения дисковых приводов), изменяются способ физического представления потока битов, лежащего в основе документированной информации (например, использование кодов с коррекцией ошибок) и конструктивные параметры (form factor) носителей. Как следствие, со временем более старые носители информации становятся несовместимыми с появившимися позднее носителями и оборудованием.

Стратегия обеспечения долговременной сохранности должна целенаправленно решать проблему устаревания носителей, устанавливая процедуры периодически выполняемого переноса документов со старых носителей на более новые.

Примечание — Правильный выбор форматов данных так же важен, как и читаемость данных. Следует обратить внимание на то, что данные должны форматироваться таким образом (т. е. с использованием «технологически нейтральных» форматов), чтобы в будущем пользователи могли эти данные обрабатывать.

5.2.3 Интерпретируемость электронных документов

Стратегия долговременной сохранности должна обеспечить возможность правильной интерпретации и отображения электронных документов. Электронная информация «понятна» (intelligible) компьютеру только тогда, когда ему также доступны сведения о том, как интерпретировать лежащий в основе этой информации поток битов. Возможность интерпретировать электронные документы зависит, таким образом, от наличия сведений о том, представлением какого объекта является поток битов, и от способности обрабатывающего информацию программного обеспечения на основе этих сведений выполнить соответствующие действия.

Пример — Двоичный код (из нулей и единиц), из которого состоит графический образ в формате TIFF, сам по себе не может быть правильно интерпретирован. Однако наличие заголовка файла, содержащего такие сведения, как информация о порядке байтов и об использованном алгоритме сжатия, позволяет компьютеру (используя совместно возможности операционной системы и программного обеспечения для работы с графическими образами) показать и распечатать изображение. Так и документ, подготовленный в текстовом редакторе, содержит метаданные, делающие его «понятным» для программы обработки текстов.

5.2.4 Идентифицируемость электронных документов

Стратегия долговременной сохранности должна обеспечить идентифицируемость электронных документов. Идентифицируемые электронные документы должны быть организованы, классифицированы и описаны таким образом, чтобы дать возможность пользователям и информационным системам различать информационные объекты на основе уникального атрибута, такого как имя или идентификационный номер. Группировка (aggregating) электронных документов по категориям на основе общих атрибутов упрощает поиск и извлечение информации. Отсутствие подобной идентификации резко ограничивает возможности поиска и извлечения информации.

5.2.5 Доступность электронных документов

Стратегия долговременной сохранности должна обеспечить доступность документов. Это означает, что отдельные информационные объекты (или их части) могут быть извлечены и показаны. Доступность обычно зависит от программного обеспечения, поскольку для ее реализации требуется знание ключей или указателей, устанавливающих связь между логической структурой информационных объектов (например, полями данных или текстовыми строками) и их физическим местоположением.

Примерами таких связей являются запись в базе данных, структура каталогов файловой системы, таблица размещения файлов (file allocation table), заголовки или метки, содержащие сведения, позволяющие определить начало объекта и число байтов в каждом компоненте или элементе данных, а также определить их физическое местоположение на носителе информации.

Интерпретация логической структуры документов является функцией операционной системы или драйвера устройства, работающих совместно с определенной прикладной системой, разработанной для хранения, управления и предоставления доступа к электронной информации. Таким образом, доступность информационных объектов неразрывно связана с драйверами устройств, программными приложениями, файловыми и операционными системами.

Новые поколения файловых форматов, поддерживающие читаемость более старых форматов, способствуют обеспечению доступности электронных документов. Обратная совместимость (совмес-

тимость «сверху вниз» — backward compatibility) с предыдущими версиями может, однако, оказаться ограниченной, поскольку многие поставщики программного обеспечения поддерживают лишь некоторые файловые форматы, в то время как другие поддерживают все версии различных форматов данных. Примером может служить поддержка данных в форматах TIFF, JPEG и HTML, обеспечивающая совместимость «сверху вниз».

5.2.6 Понятность электронных документов

Стратегия долговременной сохранности должна обеспечить возможность понять смысл документов. Чтобы электронные документы были понятными, и компьютер, и человек должны быть способны воспринимать содержащуюся в них информацию. Значение отдельного документа не определяется одним лишь его содержанием (контентом), оно, скорее, устанавливается из контекста его создания и использования (т. е. на основе метаданных). В связи с этим хранители информации должны осознавать, что обеспечение понятности электронных документов кардинально отличается от решения той же задачи в отношении бумажной документации. В отличие от бумажной документации, где ее физические характеристики обычно передают контекст создания и использования, контекст создания и использования электронных документов обычно связан с ними логически, а не на физическом уровне.

Пример — Если набор бумажных документов, относящихся к определенной транзакции, можно скрепить степлером или положить в папку «Дело», то электронные документы по такой же транзакции могут располагаться на нескольких носителях, находящихся в нескольких местах, и, следовательно, должны собираться воедино электронным образом. Соответствующие логические связи могут включать идентификацию как деловых процессов, приведших к данной транзакции, так и участников транзакции.

Контекст создания и использования включает также связи с другими документами. Для фиксации этих связей могут использоваться различные способы, включая ссылки в профиле («карточке») документа на другой документ по тому же вопросу или классификационный код, объединяющий все документы, относящиеся к одной и той же транзакции.

Успешное извлечение сохраненных электронным образом документов, таким образом, отчасти зависит от сохранения этих логических связей (независимо от давности их установления).

5.2.7 Аутентичность электронных документов

5.2.7.1 Общие положения

Ключевой задачей стратегии долговременной сохранности является обеспечение аутентичности документов. Аутентичные электронные документы — это документы, которые являются именно тем, чем они претендуют быть, т. е. это надежная информация, которая не была искажена, изменена или как-либо иначе испорчена с течением времени. Организации, стремящиеся обеспечить долговременный доступ к аутентичным документам, должны обратить внимание на следующие три ключевые аспекта своей стратегии:

a) передача/прием на хранение и ответственное хранение;

b) среда хранения;

c) управление доступом и защита.

5.2.7.2 Передача/прием на хранение и ответственное хранение документов

Пока электронные документы остаются в среде их создания (production environment) и не сохранены на защищенных от внесения изменений носителях однократной записи, их трудно защитить от модификации. Соответственно, стратегия долговременной сохранности должна предусматривать передачу документов из среды их создания и от их создателей и получателей — в систему хранения либо хранителю информации (т. е. независимой в оперативном отношении третьей стороне, на которую возложена обязанность поддержания документов в соответствии с документированными политикой и практикой).

5.2.7.3 Среда хранения

Поскольку неблагоприятные или плохо контролируемые условия среды хранения подвергают информацию риску, в стратегии долговременной сохранности должно быть предусмотрено создание стабильной среды хранения носителей информации, содержащих электронные документы.

5.2.7.4 Управление доступом и защита документов

В стратегии долговременной сохранности должны быть предусмотрены механизмы ограничения доступа к электронным документам и защиты их от случайного или умышленного искажения и порчи.

Электронные документы, сохраняемые на перезаписываемом носителе, можно модифицировать, не оставив каких-либо физических следов. Они также уязвимы в отношении случайной порчи в процессе передачи между носителями и информационными системами. Ввиду этого организациям, стремящимся обеспечить аутентичность электронных документов во времени, следует разработать

соответствующие политику, практику и технические меры контроля и управления. Примерами широко используемых технических мер являются:

- использование магнитных или оптических носителей однократной записи типа WORM (т. е. неперезаписываемых);

- применение защищенной клиент-серверной архитектуры, которую можно использовать для блокирования непосредственного доступа к электронным документам и которая в итоге позволяет организовать доступ «только на чтение»;

- использование циклического избыточного кода CRC (контрольных сумм CRC) — распространенный метод обеспечения надежности электронной передачи данных. Контрольные суммы CRC особенно полезны для подтверждения того, что никакие изменения не были внесены в электронные документы с момента их первоначального сохранения;

- применение односторонних хэш-функций (например, SHA-1), использующих алгоритм, позволяющий сжать электронные документы до фиксированного числа битов. Эти биты фактически являются уникальным «дактилоскопическим отпечатком» соответствующих документов, их впоследствии можно использовать для доказательства того, что информация не была изменена.

6 Элементы стратегии долговременной сохранности

6.1 Общие положения

Поддержание точности, надежности и достоверности электронных документов означает обеспечение того, что:

- документ может быть прочитан и правильно интерпретирован прикладной компьютерной программой;

- документ может быть представлен в виде, понятном человеку;

- документ сохраняет ту же логическую и физическую структуру, контент и контекст, которые имелись на момент его создания или получения.

Ограниченность срока службы электронных носителей информации и неизбежное технологическое устаревание будут вынуждать хранителей информации, ответственных за обеспечение долговременной сохранности аутентичных и пригодных к использованию (processable) электронных документов, принимать ключевые решения, связанные с обеспечением долговременного доступа к информации. При этом хранителям информации придется использовать различные стратегии и средства. Концептуально эти стратегии и средства можно разделить на три основных вида деятельности, которые совместно образуют фундамент любой стратегии долговременной сохранности.

a) Во-первых, для решения проблемы ограниченности срока службы носителей хранители информации должны проводить обновление носителей (см. 6.2).

b) Во-вторых, при наличии соответствующих автоматизированных средств миграция документов (см. 6.4) путем их перемещения с одной технологической платформы на другую является подходящим способом решения проблемы технологического устаревания.

c) В-третьих, в тех случаях, когда электронная информация и графические образы хранятся в унаследованных информационных системах, не имеющих автоматизированных средств для миграции, возможно, придется использовать более прямолинейный метод — эмуляцию унаследованной информационной системы на базе имеющейся технологической среды. Хотя такой вариант действий весьма привлекателен, до настоящего времени на пути его использования для долговременного доступа к аутентичным электронным документам возникали существенные препятствия. Поэтому в настоящем стандарте эмуляция не рассматривается.

6.2 Обновление носителей

6.2.1 Общие положения

Из-за ограниченности срока службы носителей информации и вследствие их технологического устаревания периодическое обновление носителей представляется, с одной стороны, неизбежным, а с другой — является базовым требованием при обеспечении долговременной сохранности аутентичной и пригодной к использованию электронной документации за счет сохранения оригинального потока битов «в живом состоянии». При обновлении носителей электронные документы придется либо переформатировать, либо скопировать, как описано в 6.2.2 и 6.2.3.

6.2.2 Переформатирование электронных документов

6.2.2.1 Общие положения

В случае переформатирования документов лежащий в их основе поток битов изменяется вследствие того, что он переносится на другой физический носитель (например, с 18-дорожечного носителя информации на носитель с 36 дорожками для записи), либо вследствие изменения кодировки символов (например, с 7-битовой на 8-битовую кодировку ASCII), но при этом не происходит никаких изменений ни в его физическом представлении, ни в контенте. Переформатирование происходит независимо от программного приложения, в котором был создан документ.

6.2.2.2 Ситуации, в которых может потребоваться переформатирование

Организациям стоит подумать о переформатировании электронных документов в следующих ситуациях:

a) *при передаче на хранение:* при передаче электронных документов хранителю информации они должна быть преобразованы в стандартную кодировку (encoding representation) и перенесены на носитель стандартного типа;

b) *при обновлении оборудования:* переформатирование оправдано, когда хранитель информации модифицирует свое оборудование и заменяет существующие устройства хранения информации на новые;

c) *при плановом переформатировании:* переформатирование планируется таким образом, чтобы совпасть с моментом истечения расчетного срока службы используемых носителей информации и/или расчетным сроком службы устройства или привода, необходимого для работы с носителями информации.

6.2.2.3 Выбор носителей информации при переформатировании

При переформатировании электронных документов хранители информации должны обдумать выбор носителей информации. В первую очередь организация должна выбрать между магнитными и оптическими технологиями. Следует учесть следующие факторы:

- большая емкость носителя;
- высокая скорость передачи информации;
- ожидаемый срок службы носителя не менее 20 лет;
- устоявшееся и стабильное присутствие на рынке носителей;
- доступность по цене;
- пригодность (suitability) соответствующей технологии для обеспечения долговременной сохранности и доступности.

Большая емкость носителей и высокая скорость передачи информации являются ключевыми факторами, поскольку в конечном итоге именно они определяют время, требуемое для переноса электронных документов в ходе переформатирования и копирования. Затраты времени с большой вероятностью могут стать проблемой при переформатировании, если объем электронной информации в хранилище будет измеряться терабайтами и петабайтами.

6.2.2.4 Переформатирование и аутентичность

После переформатирования аутентичность электронных документов может быть поставлена под сомнение, особенно если переформатирование проводилось несколько раз. Для обеспечения необходимого уровня аутентичности в системах хранения и у хранителей информации должна быть реализована документированная политика контроля качества, предписывающая обязательную проверку точности всех переформатированных документов.

Процедуры, реализующие на практике эту политику, должны включать в себя детальное и полное документирование всех действий, выполненных при переформатировании. Документироваться, в частности, должны:

- идентификация лица (лиц), фактически выполнивших процесс переформатирования;
- дата переформатирования;
- формат данных;
- сравнение контрольных сумм CRC или хэш-дайджестов, вычисленных до и после переформатирования, доказывающее отсутствие каких-либо изменений;
- результат визуального сравнения нескольких образцов переформатированных документов с соответствующими документами в старом формате.

Хорошая практика работы должна обеспечить выявление неточностей и неустранимых ошибок, а также документирование того, как эти проблемы впоследствии решались. Должно быть зафиксировано физическое местоположение обнаружения неустранимой ошибки (например, номер блока или сектора на дорожке). Кроме того, эти действия должны анализироваться третьей стороной, чтобы удостовериться в их выполнении в соответствии с установленными процедурами. Наконец, такая документация,

фиксирующая все выявленные проблемы, должна быть четко идентифицирована с указанием конкретных ссылок на соответствующие документы, и она должна рассматриваться как метаданные, заслуживающие столь же бережного отношения, как и сами документы.

6.2.2.5 Защита документов во время переформатирования

Хранители информации должны обеспечить во время переформатирования защиту электронных документов от утраты и от внесения изменений. Электронные носители информации уязвимы по отношению к вмешательству человека, катастрофическим сбоям и природным катастрофам. В связи с этим хранители информации должны предпринять следующие меры для минимизации рисков по безопасности:

- установить межсетевой экран («брандмауэр») или одностороннюю связь (например, так называемый «воздушный зазор» — «air gap»), которые разрешают доступ только на чтение и только авторизованным лицам;
- хранить электронные носители информации в запираемом, охраняемом помещении или защищенном хранилище (vault) с контролируемым доступом;
- создать резервные копии носителей информации и хранить их в другом месте, географически удаленном от места хранения оригиналов;
- желательно использовать два различных типа носителей информации для хранения оригиналов и резервных копий, чтобы минимизировать риск неожиданного технологического устаревания.

6.2.3 Копирование электронных документов

6.2.3.1 Общие положения

Цель копирования электронных документов заключается в поддержании их аутентичности и пригодности к использованию путем перемещения со старых носителей информации на новые носители с теми же спецификациями формата, без каких-либо потерь структуры, контента или контекста. Лежащий в основе электронных документов поток битов остается неизменным при копировании на новые носители информации.

6.2.3.2 Ситуации, в которых может потребоваться копирование

Копирование электронных документов может проводиться в следующих ситуациях:

- *при передаче на хранение:* электронные документы следует скопировать при их передаче хранителям информации, использующим носители с теми же спецификациями формата, что и носители, применявшиеся до передачи;
- *в случае появления ошибок при работе с носителем*: электронные документы следует скопировать, если при ежегодной выборочной проверке носителей информации на читаемость будут выявлены неустранимые ошибки или большое число «временных» ошибок чтения, но при этом не возникнет необходимости в переходе на новый тип носителей или устройств чтения;
- *при плановом копировании:* электронные документы следует скопировать, если носители информации «состарились», но при этом не возникло необходимости в переходе на новый тип носителей или устройств чтения, поскольку используемые варианты по-прежнему широко поддерживаются и удовлетворяют функциональным требованиям, предъявляемым организацией. Организациям следует установить фиксированный период времени (например, равный половине ожидаемого срока службы носителей), по истечении которого проводится копирование электронных документов на новые носители информации.

6.2.3.3 Сохранение аутентичности при копировании

Хотя поток составляющих документы битов при копировании не изменяется, все же остается потенциальная возможность порчи данных в ходе процесса копирования. Для обеспечения необходимого уровня аутентичности у хранителей информации должна быть реализована документированная политика контроля качества, предписывающая обязательную проверку точности всех скопированных документов.

Процедуры, реализующие на практике эту политику, должны включать в себя детальное и полное документирование всех действий, выполненных при копировании. Документироваться, в частности, должны:

- идентификация лица (лиц), фактически выполнившего(их) процесс;
- дата копирования;
- формат данных;
- число обработанных битов/байтов;
- сравнение контрольных сумм CRC или хэш-дайджестов, вычисленных до и после копирования, доказывающее отсутствие каких-либо изменений;
- результат визуального сравнения нескольких образцов скопированных документов с соответствующими документами на старом носителе.

Хорошая практика работы должна обеспечить выявление неточностей и неустранимых ошибок и документирование того, как эти проблемы впоследствии решались. Должно быть зафиксировано физическое местоположение обнаружения неустранимой ошибки (например, номер блока или сектора на дорожке). Кроме того, эти действия должны анализироваться третьей стороной, чтобы удостовериться в их выполнении в соответствии с установленными процедурами. Наконец, такая документация, фиксирующая все выявленные проблемы, должна быть четко идентифицирована с указанием конкретных ссылок на соответствующие документы, и она должна рассматриваться как метаданные, заслуживающие столь же бережного отношения, как и сами документы.

6.2.3.4 Защита документов во время копирования

Хранители информации должны обеспечить во время копирования защиту электронных документов от утраты и от внесения изменений. Электронные носители информации уязвимы по отношению к вмешательству человека, катастрофическим сбоям и природным катастрофам. В связи с этим хранители информации должны предпринять следующие меры для минимизации рисков по безопасности:

- установить межсетевой экран («брандмауэр») или одностороннюю связь (например, так называемый «воздушный зазор» — «air gap»), которые разрешают доступ только на чтение и только авторизованным лицам;
- хранить электронные носители информации в запираемом, охраняемом помещении или защищенном хранилище (vault) с контролируемым доступом;
- провести сравнение контрольных сумм CRC или хэш-дайджестов, вычисленных до и после копирования, доказывающее отсутствие каких-либо изменений;
- создать резервные копии носителей информации и хранить их в другом месте, географически удаленном от места хранения оригиналов;
- желательно использовать два различных типа носителей информации для хранения оригиналов и резервных копий, чтобы минимизировать риск неожиданного технологического устаревания.

6.3 Метаданные

6.3.1 Общие положения

Метаданные (данные о данных) включают в себя информацию о контексте, обработке и об использовании данных, которая используется при идентификации, извлечении и обеспечении сохранности аутентичных электронных документов.

В одних случаях определенные программные приложения могут автоматически создавать метаданные, такие как размер файла, формат файла, дата, хэш-дайджест и другие аналогичные атрибуты (например, свойства электронных документов и т. п.), в других — может потребоваться ручной ввод таких метаданных, как, например, классификация, срок хранения, индекс по номенклатуре дел или ключевые слова. Как и электронные документы, эти данные могут быть доступными.

Весьма вероятно, что по мере внедрения организациями корпоративных систем управления контентом состав элементов метаданных, применимых для реализации стратегии долговременной сохранности, станет гораздо «богаче» чем сейчас. Помимо этого, метаданные, скорее всего, будут создаваться автоматически, и отпадет необходимость в их ручном вводе. Учитывая все это, хранители информации должны позаботиться о том, чтобы применяемые ими средства сбора и использования метаданных были достаточно гибкими и масштабируемыми, чтобы впоследствии они могли работать с более разнообразными наборами элементов метаданных.

6.3.2 Взаимная совместимость (интероперабельность) метаданных

В будущем метаданные, имеющиеся в корпоративных системах управления контентом, будут взаимно совместимыми. Поэтому организациям, проектирующим сбор и применение метаданных, которые предполагается использовать в интероперабельной среде, следует принять во внимание ИСО 23081-1.

6.4 Миграция электронных документов

6.4.1 Общие положения

Стратегия долговременной сохранности должна включать положения, предусматривающие миграцию электронных документов.

Хранители информации, в обязанности которых входит сбор и сохранение аутентичных электронных документов, а также обеспечение доступа к ним во времени, сталкиваются с четырьмя проблемами:

а) в ближайшем будущем организации и отдельные лица будут продолжать пользоваться широким набором пакетов программ и форматов хранения данных в целях создания и использования электронных документов. Для хранителей информации, принимающих эти документы, будет чрезвычайно

сложно иметь доступ ко всему соответствующему программному обеспечению или поддерживать все эти пакеты программ и форматы;

b) часть электронных документов, вероятно, окажется зависимой от программного обеспечения, и, соответственно, их можно будет использовать только в рамках определенной программной среды;

c) операционные системы и прикладное программное обеспечение неизбежно будут вытесняться более новыми и производительными продуктами, имеющими больше функциональных возможностей. Это означает, что хранителям информации придется периодически перемещать электронные документы из текущей программной среды в новую;

d) некоторые электронные документы, вероятно, будут доступны лишь в унаследованных информационных системах, не имеющих автоматических средств миграции.

Миграция электронных документов позволяет успешно решить все эти четыре проблемы. Хранителям информации нужно будет организовать миграцию аутентичных электронных документов из среды одного программного приложения в среду нового программного приложения таким образом, чтобы не было никаких потерь контента и контекста, а также чтобы отсутствовала или была минимальной потеря структуры.

6.4.2 Зависимость от программного обеспечения

Стратегия долговременной сохранности должна решать проблему зависимости от конкретного программного обеспечения. Если электронные документы могут быть использованы только при помощи определенного программного приложения, то обеспечение долговременного доступа к этим документам может оказаться проблематичным, особенно если поставщик прекратит техническую поддержку или не обеспечит преемственность в новых версиях программного обеспечения. Во многих случаях возможно избавиться от зависимости такого рода, частично пожертвовав структурой, например, текстовые документы из первоначальной среды программного приложения для обработки текстов могут быть мигрированы в простой текст (т. е. «чистый» ASCII-текст) путем автоматического удаления встроенных инструкций форматирования или кода, управляющего определенными аспектами физического представления, такими как жирный шрифт или примечания.

Хотя такие действия и уменьшают зависимость от программного обеспечения, хранители информации должны тщательно оценить их последствия для аутентичности мигрированных подобным образом документов. Такие документы уже нельзя будет рассматривать в качестве имитационных копий (imitative copies), поскольку они не будут в точности воспроизводить структуру оригинальных документов. Скорее, получившиеся документы следует рассматривать в качестве «новых» документов, аутентичность которых должна быть установлена заново благодаря документированию всех выполненных действий и путем проверки и подтверждения неизменности контента документов.

Альтернативой миграции текстовых электронных документов в простой текст является распечатывание их на бумаге или вывод на микропленку, что позволяет сохранить аутентичность за счет удобства обработки и использования. Такой подход особенно оправдан в отношении электронных документов, аналогичных постранично организованным бумажным документам (page analog electronic records), пригодность которых к обработке и использованию в принципе может быть восстановлена в будущем за счет использования средств распознавания текста (OCR).

Таблицы иерархических и реляционных баз данных также можно мигрировать в «плоские» табличные структуры, чтобы минимизировать зависимость от программного обеспечения конкретного поставщика. В этом случае идентификация первичного ключа (primary key) и внешних ключей (foreign keys) в каждой таблице должна быть сохранена, в то время как реляционные связи удаляются. В процессе такого преобразования должны быть созданы метаданные, показывающие, какого типа были эти связи — «один к одному», «один ко многим», «многие к одному» или «многие ко многим», чтобы в будущем эти связи можно было восстановить.

6.4.3 Обновление программного обеспечения и инсталляция нового программного обеспечения

Поскольку хранителям информации, обеспечивающим долговременный доступ к аутентичным документам, неизбежно придется обновлять существующее и инсталлировать новое программное обеспечение, то стратегия долговременной сохранности должна включать политику и процедуры на этот случай.

Когда происходит обновление программного обеспечения (например, от версии 1 к версии 2) и поставщик обеспечивает обратную совместимость (совместимость «сверху вниз») обновленного и старого программного обеспечения, документы следует автоматически перевести в новую среду, вместе с лежащей в их основе схемой физического представления (underlying physical representation scheme), существенным контентом и контекстом.

В тех случаях, когда новое программное обеспечение заменяет существующее, — как автономное программное приложение или как часть общего обновления информационной системы, — следует провести миграцию документов, используя функции экспорта старой системы и функции импорта новой системы. Кроме того, в некоторых средах может поддерживаться миграция через сопряжения (gateways) импорта/экспорта, разработанные для отдельных коммерческих (проприетарных) форматов (например, преобразование из формата одного текстового процессора в формат другого).

6.4.4 Миграция в стандартные форматы

После передачи электронных документов на хранение хранителям информации следует подумать об их миграции из широкого набора форматов, используемых создателями и получателями документов, в меньшее число «стандартизованных» форматов. Выбор «стандартизованных» форматов может быть результатом консенсуса относительно широко используемых форматов, которые покрывают большую часть электронных документов определенного класса. Следует избегать коммерческих (проприетарных) форматов. К числу заслуживающих внимания технологически нейтральных форматов относятся PDF/A-1, XML, TIFF и JPEG.

6.4.5 Миграция электронных документов из унаследованных информационных систем

6.4.5.1 Общие положения

Стратегия обеспечения долговременного доступа к аутентичным и пригодным к использованию электронным документам должна предусматривать миграцию в тех случаях, когда отсутствуют как обратная совместимость, так и сопряжения экспорта/импорта между старой (унаследованной) системой, в которой хранится документация, и новой информационной системой.

В будущем потребность в миграции электронных документов из унаследованных информационных систем может сократиться вследствие более широкого распространения систем, поддерживающих архитектуры и форматы, нейтральные по отношению к используемым поставщиками технологиям. Пока, однако, хранителям информации, чтобы выполнить свои обязательства, приходится проводить миграцию электронных документов, находящихся в устаревших информационных системах.

Некоторая потеря информации во время повторяющихся циклов миграции неизбежна из-за фундаментальной несовместимости, существующей между несколькими поколениями более старых и более новых систем. Соответственно, хранителям информации, вместо того чтобы пытаться полностью избежать потерь информации, рекомендуется разработать политики миграции и процедуры контроля качества, нацеленные на уменьшение деградации информации в процессе миграции. Одной из важных процедур является документирование потерь, имевших место в ходе миграции, и результатов деятельности по контролю качества. По возможности эта документация должна сохраняться вместе с носителями информации.

6.4.5.2 Этапы миграции

6.4.5.2.1 Общие положения

Хранителям информации следует внедрить 10-этапный подход к выполнению миграции. Поскольку обстоятельства каждого отдельного проекта миграции могут существенно отличаться, описанные ниже десять этапов не должны рассматриваться как конкретный план миграции, применимый при любых обстоятельствах.

6.4.5.2.2 Анализ унаследованной информационной системы (этап 1)

Хранители информации должны провести анализ унаследованной информационной системы с целью понять, какие функции она выполняет и какие документы в ней содержатся. В ходе анализа определяются:

- обоснование выполняемых системой функций;
- способ сбора (захвата) метаданных, их взаимосвязь с документами;
- взаимосвязи между документами.

На этом этапе должен быть создан информационный продукт — спецификации, которые будут использованы при «прямом» проектировании (forward engineering) функциональных возможностей, метаданных и документов для новой системы.

6.4.5.2.3 Декомпозиция структуры унаследованной информационной системы (этап 2)

Хранителям информации следует провести декомпозицию унаследованной информационной архитектуры, чтобы с ее интерфейсами, приложениями и сервисами базы данных можно было работать как с отдельными компонентами (это, однако, возможно сделать не для всех информационных систем):

- декомпозиция унаследованной системы возможна, если системные и пользовательские интерфейсы, модули программных приложений, сервисы базы данных и сама база данных являются отдельными и независимыми компонентами;

- унаследованная система частично поддается декомпозиции, если интерфейсы и база данных являются независимыми, а программное приложение и сервисы базы данных составляют единый модуль;

- унаследованная система не поддается декомпозиции, если интерфейсы, приложения и сервисы базы данных объединены в одном модуле.

В любом случае при подготовке к миграции должны быть устранены все внешние зависимости в архитектуре системы.

6.4.5.2.4 Проектирование интерфейсов новой системы (этап 3)

Должна быть обеспечена связь (преемственность) между новыми и старыми интерфейсами.

6.4.5.2.5 Проектирование новых программных приложений (этап 4)

Должна быть обеспечена связь (преемственность) между новыми и старыми программными приложениями.

6.4.5.2.6 Проектирование новых баз данных (этап 5)

Должна быть обеспечена связь (преемственность) между новыми и унаследованными базами данных.

6.4.5.2.7 Инсталляция и всестороннее тестирование новой среды (этап 6)

Необходимо идентифицировать, выбрать, инсталлировать и полностью протестировать открытую новую среду (имеющую соответствующие средства инсталляции).

6.4.5.2.8 Разработка и инсталляция необходимых модулей сопряжения (gateways) (этап 7)

Для обеспечения согласованности и точности в воспроизведении функциональных возможностей унаследованной системы в новой системе и для перемещения электронных документов следует спроектировать, разработать и инсталлировать модули сопряжения (gateways). Такие модули обычно выполняют две функции. Первая — изоляция определенных компонентов от влияния изменений, вносимых в другие компоненты, вторая — функционирование в качестве преобразователя запросов и данных, которыми обмениваются обслуживаемые сопряжением компоненты. Для обеспечения согласованности и точности модули сопряжения должны быть тщательно протестированы на образцах документов из унаследованной системы.

6.4.5.2.9 Миграция унаследованной базы данных (этап 8)

Должна быть проведена миграция унаследованной базы данных в новую базу данных.

6.4.5.2.10 Миграция унаследованных программных приложений (этап 9)

Должна быть проведена миграция унаследованных программных приложений в новые программные приложения.

6.4.5.2.11 Миграция унаследованных интерфейсов (этап 10)

Должна быть проведена миграция унаследованных интерфейсов в новые. Унаследованные интерфейсы (например, текстовые меню и экраны) будут, скорее всего, заменяться графическими интерфейсами.

7 Разработка стратегии долговременной сохранности

7.1 Политика обеспечения долговременной сохранности

Хранители информации, стремящиеся обеспечить долговременную сохранность аутентичных и пригодных к использованию электронных документов, должны подготовить документацию, описывающую их политику и процедуры. Такая документация послужит дополнительным подтверждением аутентичности электронных документов при их использовании в качестве свидетельств (доказательств) и поможет обеспечить согласованность и единообразие их обработки. Кроме того, такая документация поможет хранителю информации давать ответы на вопросы о достоверности документов, которые обычно поднимаются в ходе судебных разбирательств.

Политика, направленная на реализацию стратегии долговременной сохранности, должна включать:

- раздел, содержащий положение о том, что обеспечение долговременной сохранности аутентичных и пригодных к использованию документов является целью хранителя информации, а также перечень других целей и обязанностей хранителя;

- описание вида ответственности за хранение (custody), которую хранитель информации берет на себя в отношении электронных документов, например законное попечение (legal custody) или ответственное физическое хранение (physical custody);

- описание хорошей практики управления электронными документами, которой придерживается хранитель информации;

- указание обстоятельств, при которых будут проводиться действия по миграции, а также соответствующие методы и обоснования этих действий;
- описание видов аудита, которые предполагается проводить, на соответствие установленным требованиям;
- разъяснение ролей, исполняемых персоналом хранителя информации, и описание всех обязанностей, передаваемых на аутсорсинг.

7.2 Контроль качества

Аутентичность электронных документов, сохраняемых в соответствии с установленными правилами и процедурами, обычно более доказуема, и такие документы вызывают большее доверие в случае судебных разбирательств и расследований.

Исходя из этого, хранителям информации следует внедрить политики и хорошие практики для каждого осуществляемого ими вида деятельности.

Свидетельства, показывающие, каким образом осуществлялось управление электронными документами, могут оказаться ключевыми в случае судебных разбирательств, поэтому к ним следует относиться так же бережно, как и к переданным под ответственность хранителя информации электронным документам. К числу таких свидетельств принадлежат все соответствующие политики и процедуры, документация, отражающая любые потери данных в ходе миграции, и результаты периодически проводимых аудитов в области контроля качества, целью которых является обеспечение исполнения этих политик и процедур.

7.3 Безопасность

7.3.1 Общие положения

Защита электронных документов от модификации, внесения изменений и от утраты является важнейшей задачей хранителя информации, обязанностью которого является обеспечение долговременного доступа к аутентичным и пригодным к использованию электронным документам. В связи с этим хранителям информации для исполнения своих обязательств следует применять меры, описанные в 6.2.2.3.

7.3.2 Управление доступом при помощи программных средств

Хранители информации должны использовать описанные ниже автоматизированные процедуры для контроля над операциями модификации и/или уничтожения электронной информации.

Сведения о модификации/уничтожении каких-либо электронных документов, включающие имя сотрудника и причину модификации/уничтожения, должны автоматически протоколироваться прикладной программой/программным обеспечением.

В целях предотвращения несанкционированного доступа к электронным документам доступ к ним должен осуществляться только посредством использования документированного программного обеспечения/программных приложений, прошедших тщательное тестирование и проверку.

По завершении каждой операции модификации/уничтожения вся соответствующая контрольная информация (history and logging information) должна сохраняться на защищенных от внесения изменений носителях однократной записи.

7.3.3 Управление физическим доступом

Хранители информации должны применять следующие меры для контроля над физическим доступом к электронным документным системам:

- доступ в помещение хранилища должен разрешаться только авторизованному персоналу;
- должен вестись журнал прибытия/убытия, в котором должны регистрироваться дата, время и фамилия каждого лица, входящего в охраняемое помещение хранилища;
- в случае изъятия авторизованным персоналом носителей информации должен быть составлен документ, содержащий дату, время и краткое описание причины изъятия;
- руководители, на которых возложены контрольные функции, должны периодически проверять журналы, для того чтобы убедиться в исполнении персоналом установленных требований. Сами журналы должны сохраняться в качестве доказательства того, что организация соблюдает требования собственных политик.

7.3.4 Защита от утраты

Хранители информации должны применять следующие меры для защиты электронных документов от утраты:

- хранилище информации должно располагаться в таком месте, где угроза природных катастроф (например, наводнения, пожара, землетрясения или падения метеорита) минимальна;
- хранилище информации должно быть оборудовано системами обнаружения и тушения пожара;

- должен иметься полномасштабный план восстановления деятельности после катастроф, включающий категоризацию электронных документов, чтобы была возможность устанавливать приоритеты при спасении и восстановлении носителей информации;
- хранитель информации, использующий магнитные носители, должен располагать помещения своих хранилищ вдали от неэкранированных мощных электромоторов (используемых, например, в системах кондиционирования воздуха), генераторов, трансформаторов и высоковольтных линий электропередач.

7.3.5 Политика обеспечения безопасности

Хранители информации должны разработать документированные процедуры обеспечения безопасности, в которых должны быть описаны:

- меры безопасности, применяемые при передаче электронных документов хранителю информации;
- процедуры управления доступом и порядок контроля выполнения этих процедур;
- местоположение помещения хранилища, выбранное таким образом, чтобы минимизировать угрозу утраты информации вследствие природных катастроф;
- план по восстановлению деятельности после катастроф;
- заявление о соблюдении общепризнанных стандартов, касающихся порядка обращения с носителями информации;
- меры по созданию вспомогательного (резервного) хранилища для хранения резервных копий носителей информации и для выполнения процедур, связанных с восстановлением деятельности в организации в случае катастроф.

7.4 Контроль и мониторинг климатических условий

«Хрупкость» электронных носителей информации создает риск для их читаемости и продолжительности срока службы. В связи с этим хранителям информации следует внедрить программу контроля и мониторинга климатических условий, которая должна включать следующие меры:

- создание среды хранения, в которой температура и относительная влажность поддерживаются в соответствующем диапазоне, установленном общепризнанными стандартами и/или по результатам авторитетных исследований;
- использование системы фильтрации воздуха, удаляющей из среды хранения частицы пыли и газообразные загрязнения;
- запрет на курение и употребление пищи и напитков в зоне хранения;
- реализация программы, в рамках которой ежегодно проводится проверка на читаемость статистической выборки из общего числа электронных документов с целью выявления имеющей место или возможной потери информации.

Приложение А
(справочное)

Национальные программы обеспечения сохранности электронных документов и другие публикации

А.1 Общие положения

Приведенные в данном приложении сведения даны исключительно для справки. Они не являются исчерпывающими, и пользователи сами должны подобрать подходящие им методические документы.

Раздел А.2 включает избранные национальные программы в области обеспечения сохранности электронных документов, имеющие отношение к данному стандарту.

Раздел А.3 содержит публикации по тематике настоящего стандарта, раздел А.4 — стандарты ИСО.

А.2 Национальные программы обеспечения сохранности электронных документов

[1] Австралия: «Зеленая книга», выпущенная Национальными Архивами Австралии, «Метод обеспечения сохранности электронных документов» (An Approach to the Preservation of Digital Records), 1999.

[2] Голландия: «Тестовый стенд по обеспечению сохранности цифровой информации. Миграция: Контекст и текущее состояние» (Digital Preservation Testbed. Migration: Context and Current Status), Национальные Архивы Голландии, 2001.

[3] Франция: «Электронные архивные документы. Практическое руководство» (Les archives électroniques. Manuel pratique), Дирекция архивов Франции, 2002.

[4] ЮАР: «Руководство по управлению электронными документами в государственных органах» (Guide to the Management of Electronic Records in Governmental Bodies), Национальные Архивы Южной Африки, 2-е издание, Претория, 2000.

[5] Великобритания: «Руководство по управлению, экспертизе ценности и сохранению электронных документов», том II, Процедуры, глава 5 «Обеспечение сохранности электронных документов» (Guidelines for the Management, Appraisal and Preservation of Electronic Records. Vol. II, Procedures, Ch. 5 “Preserving Electronic Records”), Национальные Архивы Великобритании, 1999.

[6] США: Свод федеральных нормативных актов, часть 36, глава XII-B, раздел 1234 «Управление электронными документами» (36 Code of Federal Regulations, Chapter XII, Subchapter B, Part 1234, “Electronic Records Management”), Национальные Архивы США.

А.3 Публикации по тематике настоящего стандарта

[1] AMBACHER, B. I. ed. Thirty Years of Electronic Records, Scarecrow Press, 2003

[2] BEARMAN, D. Reality and chimeras in the preservation of electronic records, D-Lib Magazine, 5 (4), April 1999

[2] DOLLAR, C.M. Authentic Electronic Records: Strategies for Long-Term Access, Cohasset Associates, 1999

[3] DOLLAR, C.M. Selecting Storage Media for Long-Term Access to Digital Records, in The Information Management Journal, Vol. 33 No. 3 (July 1999)

[4] DURANTI, L., EASTWOOD, T. and MACNEIL H. Preservation of the Integrity of Electronic Records, Dordrecht: Kluwer Academic Publishers Group, 2002

[5] EVANS, J. and LINDBERG, L. Describing and analyzing the recordkeeping capabilities of metadata sets

[6] HEDSTROM, M. Digital preservation: a time bomb for digital libraries, Computers and the Humanities, 31 (3), 1997, pp. 189—202

[7] HUNTER, G.S. Preserving Digital Information, A How-To-Do-It Manual, New York: Neal-Schuman Publishers, Inc., 2000

[8] LAVOIE, B.F. Technology Watch Report. The Open Archival Information System Reference Model: Introductory Guide, публикация доступна в электронном виде по адресу gost.e-ecolog.ru

[9] LEE, KYONG-HO, SLATTELRY, O.R., LU, XIA TANG and MCCRARY, V. The State of the Art and Practice in Digital Preservation, Journal of Research of the National Institute of Standards and Technology, (Jan-Feb 2002)

[10] ROTHENBERG, J. Avoiding Technological Quicksand: Finding a Viable Technical Foundation for Digital Preservation: A Report to the Council on Library and Information Resources, Washington, DC: Council on Library and Information Resources, January 1999

[11] SPROULL, R.F. and EISENBERG, J., (eds), Building an Electronic Records Archive at the National Archives and Records Administration: Recommendations for Initial Development, Washington, DC: Computer Science and Telecommunications Board, National Academies of Science, 2003

[12] THIBODEAU, K. Overview of Technological Approaches to Digital Preservation in the Coming Years, in The State of Digital Preservation: An International Perspective. Conference Proceedings. Washington, DC: Council on Library and Information Resources, April 2002

[13] VAN BOGART, J. 1996 Media Stability Studies, National Media Laboratory, 1996

А.4 Стандарты ИСО

[1] ИСО 11799 «Информация и документация — Требования по организации хранения архивных и библиотечных материалов» (Information and documentation — Document storage requirements for archive and library materials)

[2] ИСО 14721:2003 «Системы передачи космических данных и информации — Открытые архивные информационные системы — Базовая модель» (Space data and information transfer systems — Open archival information system — Reference model)

[3] ИСО 15801:2004 «Управление электронными графическими образами — Информация, сохраняемая электронным образом — Рекомендации по обеспечению надежности и достоверности» (Electronic imaging — Information stored electronically — Recommendations for trustworthiness and reliability)

[4] ИСО/МЭК 27002 «Информационные технологии — Методы безопасности — Руководство по управлению безопасностью информации» (Information technology — Security techniques — Code of practice for information security management)

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов и документов ссылочным национальным стандартам Российской Федерации

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО 12651:1999	—	*
ИСО 15489-1	IDT	ГОСТ Р ИСО 15489-1—2007 «Система стандартов по информации, библиотечному и издательскому делу. Управление документами. Общие требования»
ИСО/ТО 15489-2	—	*
ИСО/ТУ 23081-1	IDT	ГОСТ Р ИСО 23081-1—2008 «Система стандартов по информации, библиотечному и издательскому делу. Процессы управления документами. Метаданные для документов. Часть 1. Принципы»

* 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 — идентичный стандарт.

УДК 651.9:004:006.3 ОКС 37.080:25.040.40

Ключевые слова: управление документацией, информация в электронном виде, хранение информации, сохранность информации, сохранность электронных документов, долговременная сохранность электронных документов

Редактор *Н.В. Авилочкина*
Технический редактор *Н.С. Гришанова*
Корректор В.Е. Нестерова
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 30.04.2013. Подписано в печать 03.06.2013. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,35. Тираж 113 экз. Зак. 583.

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