
ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р ИСО
14641–

Управление электронными документами

**ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ
ИНФОРМАЦИОННОЙ СИСТЕМЫ
ДЛЯ ОБЕСПЕЧЕНИЯ ДОЛГОВРЕМЕННОЙ
СОХРАННОСТИ ЭЛЕКТРОННЫХ
ДОКУМЕНТОВ**

Технические требования

(ISO 14641:2018, IDT)

Настоящий проект стандарта не подлежит применению до его утверждения



Москва
Стандартинформ
2019

Предисловие

1 ПОДГОТОВЛЕН Обществом с ограниченной ответственностью «ЭОС Тех» на основе собственного перевода на русский язык англоязычной версии 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 №

4 Настоящий стандарт идентичен международному стандарту ИСО 14641:2018 «Управление электронными документами. Проектирование и эксплуатация информационной системы для обеспечения долговременной сохранности электронных документов. Технические требования» (ISO 14641:2018 Electronic document management – Design and operation of an information system for the preservation of electronic documents – Specifications, IDT).

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

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года)

информационном указателе «Национальные стандарты», а официальный текст изменений и поправок – в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартиформ, 2019

Настоящий стандарт не может быть 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	2
3	Термины и определения	3
4	Основные характеристики и уровни требований к информационным системам ...	8
4.1	Характеристики информационных систем	8
4.2	Уровни требований	10
5	Общие требования	15
5.1	Общие положения	15
5.2	Техническое описание	15
5.3	Профили хранения	16
5.4	Процедуры оперативного использования	17
5.4.1	Общие положения	17
5.4.2	Оцифрованные документы	17
5.4.3	Изначально-электронные документы	18
5.5	Безопасность	18
5.5.1	Организация и управление безопасностью	18
5.5.2	Оценка риска	20
5.5.3	Физическая безопасность	21
5.5.4	Безопасность оборудования	21
5.5.5	Безопасность программных продуктов и заказного программного обеспечения	22
5.5.6	Техническое обслуживание информационной системы	23
5.5.7	Управление изменениями в системе и миграция носителей информации	24
5.5.8	Резервные копии	25
5.5.9	Непрерывность доступа к документам	25
5.6	Проставление отметок даты и времени	26
5.7	Контрольная информация	28
5.7.1	Общие положения	28
5.7.2	Защищённое хранение контрольной информации	28
5.7.3	Журнал аудита жизненного цикла документального фонда	29
5.7.4	Журнал событий	30
6	Носители информации	31
6.1	Характеристики носителей информации	31
6.2	Обеспечение долговременной сохранности архивных носителей информации	32
7	Системы, использующие съёмные носители	33
7.1	Общие положения	33
7.2	Инициализация логических томов на съёмных носителях	34
7.3	Закрытие логических томов на съёмных носителях	34
7.4	Маркировка физических WORM-носителей информации	34
8	Системы, использующие логические WORM-носители	35
9	Системы, использующие перезаписываемые носители информации	35
9.1	Общие положения	35

9.2	Стандартный уровень безопасности.....	36
9.3	Усиленный уровень безопасности.....	37
9.4	Продвинутый уровень безопасности.....	37
10	Процессы ввода/захвата документов в систему хранения	38
10.1	Документы в электронном виде	38
10.1.1	Общие положения	38
10.1.2	Процедура ввода документов в систему хранения	38
10.1.3	Электронные документы, структурированные с помощью языка разметки	39
10.1.4	Электронные документы в формате представления документов	39
10.1.5	Другие форматы электронных документов	40
10.1.6	Потоки печати	40
10.1.7	Проверка электронных документов	41
10.1.8	Контроль целостности электронных документов, передаваемых из исходных программных приложений	41
10.1.9	Сбор/захват метаданных	41
10.1.10	Индексирование и поиск документов	42
10.2	Бумажные документы и документы на микроформах	43
10.2.1	Средства оцифровки/сканирования документов	43
10.2.2	Средства обработки изображений	43
10.2.3	Процедура захвата бумажных документов и документов на микроформах	45
10.2.4	Контрольная информация о событиях	47
10.3	Аналоговые аудиовизуальные документы на ленточных носителях	49
10.3.1	Общие положения	49
10.3.2	Подготовка исходных ленточных носителей	49
10.3.3	Оцифровка аудио- и аудиовизуальных документов	49
10.3.4	Обработка аудио- и аудиовизуальной информации	50
10.3.5	Контрольная информация о событиях	51
10.4	Методы сжатия графических образов, звуковой и аудиовизуальной информации	53
10.4.1	Виды сжатия	53
10.4.2	Бумажные документы и документы на микроформах	53
10.4.3	Аудиовизуальные документы	54
10.5	Преобразование (конверсия) форматов	55
11	Операции с хранимыми документами	56
11.1	Область применения	56
11.2	Доступ	57
11.2.1	Общие положения	57
11.2.2	Оцифрованные документы	57
11.2.3	Электронные документы, структурированные с помощью языка разметки	58
11.2.4	Электронные документы, использующие языки описания внешнего представления	58
11.3	Реституция	58
11.4	Уничтожение документов	59
12	Аудит системы хранения электронных документов	60

12.1	Общие положения.....	60
12.1.1	Общие положения об аудите.....	60
12.1.2	Цели аудита.....	60
12.1.3	Обязанности аудиторов.....	60
12.1.4	Персонал, ответственный за проведение аудита.....	61
12.1.5	Управление документацией.....	62
12.1.6	Документирование операций аудита.....	62
12.2	Внутренний аудит.....	62
12.3	Внешний аудит.....	63
13	Хранение документов доверенной третьей стороной.....	63
13.1	Деятельность доверенной третьей стороны – поставщика услуг хранения.....	63
13.2	Типовой договор об оказании услуг.....	65
13.2.1	Содержание договора об оказании услуг.....	65
13.2.2	Продолжительность оказания услуг.....	66
13.2.3	Сроки хранения документов.....	66
13.2.4	Качество оказания услуг.....	66
13.2.5	Обеспечение безопасности и защита данных.....	67
13.2.6	Информирование и консультирование.....	67
13.2.7	Переход к другому поставщику и непрерывность ответственного хранения.....	68
13.2.8	Переносимость.....	68
13.2.9	Реституция.....	69
13.2.10	Конфиденциальность и защита персональных данных.....	69
13.2.11	Страхование профессиональной ответственности.....	70
13.2.12	Субподряд.....	70
13.2.13	Аудит.....	71
14	Поставщики услуг.....	71
14.1	Общие положения.....	71
14.2	Требования к субподрядчику.....	71
14.3	Договор с субподрядчиком.....	72
14.4	Передача данных по телекоммуникационным сетям.....	72
	Приложение А (справочное) Политика хранения.....	73
	Приложение В (справочное) Декларация практики хранения документов.....	75
	Приложение С (справочное) Общие условия обслуживания.....	77
	Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации.....	78
	Библиография.....	80

Вступление

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

Процедуры, использованные для разработки настоящего документа, и процедуры, предназначенные для его дальнейшего поддержания, описаны в Части 1 Директив ИСО/МЭК. В частности, следует обратить внимание на различные критерии утверждения, применяемые в отношении различных типов документов ИСО. Настоящий документ был составлен в соответствии с редакционными правилами Части 2 Директив ИСО/МЭК (см. <https://www.iso.org/ru/directives-and-policies.html>).

Существует вероятность того, что некоторые элементы данного документа могут подпадать под действие патентного права. ИСО не несёт ответственности за идентификацию соответствующих патентных прав. Сведения о любых патентных правах, выявленных в процессе подготовки документа, приводятся во Введении и/или в перечне ИСО полученных патентных декларации (см. <https://www.iso.org/ru/iso-standards-and-patents.html>).

Любое торговое название, используемое в настоящем документе, является информацией, приведенной для удобства пользователей, и не означает одобрения или поддержки.

Разъяснение добровольного характера стандартов, значений конкретных терминов и формулировок ИСО, относящихся к оценке соответствия, а также

ГОСТ Р ИСО 14641–
(проект, первая редакция)

сведения о приверженности ИСО принципам Всемирной торговой организации (ВТО), сформулированным в Соглашении по техническим барьерам в торговле ВТО, можно найти по адресу: <https://www.iso.org/ru/foreword-supplementary-information.html>.

Настоящий документ был подготовлен подкомитетом ПК 1 «Качество, сохранность и целостность информации» Технического комитета ИСО/ТК 171 «Приложения для управления контентом».

Настоящая первая редакция отменяет и заменяет стандарт ИСО 14641-1:2012, который был содержательно пересмотрен.

Введение

Электронные документы, как создаваемые организациями и учреждениями, так и получаемые ими, являются неотъемлемым элементом повседневной деловой деятельности. Важно, чтобы электронные документы сохранялись надлежащим образом, полностью или частично, в защищенных информационных системах, предназначенных для ведения оперативной деловой деятельности и для управления документами, в целях удовлетворения законодательно-нормативных и деловых требований.

Защищенные информационные системы решают такие стоящие перед организациями задачи, как:

- а) оптимизация захвата и хранения электронных документов, обеспечение их целостности и долговременной сохранности;
- б) предоставление средств поиска информации;
- с) обеспечение удобства доступа и использования электронных документов.

Настоящий стандарт предлагает организациям базовую концепцию, описывающую методы и способы, которые следует использовать при внедрении электронной информационной системы для управления содержащимися в ней документами. В сочетании с политиками организации по вопросам управления документами и их хранения, стандарт устанавливает критерии, используемые при проектировании систем, а также требования к оперативным процессам.

Данные требования призваны обеспечить, чтобы все документы, управляемые информационной системой, захватывались, сохранялись, извлекались и делались доступными таким образом, чтобы в течение всего срока хранения сохранённый документ гарантированно являлся аутентичным представлением оригинального документа. Аутентичное представление (authentic rendition) означает, что выдаваемый документ точно соответствует исходному, каким тот был на момент ввода в информационную систему, по критериям целостности и аутентичности (верности - fidelity), и что это обеспечивается на протяжении всего срока хранения.

В стандарте рассматривается использование трех возможных видов архивных носителей информации: физических WORM-носителей однократной записи,

логических WORM-носителей и перезаписываемых носителей. Целостность информации, хранимой на физических и логических WORM-носителях однократной записи, обеспечивается свойствами, внутренне присущими WORM-решениям. В случае перезаписываемых носителей, целостность информации обеспечивается путем использования криптографических методов, в частности, путем вычисления контрольных сумм или значений хеш-функции, использования отметок даты и времени или электронной цифровой подписи. Во всех случаях необходимо соблюдать соответствующие процедуры.

В зависимости от типа сохраняемых документов, могут оказаться полезными другие специализированные стандарты, которые могут использоваться в дополнение к рекомендациям настоящего стандарта.

В настоящем стандарте ряд вопросов, по сравнению с другими стандартами и требованиями к управлению электронной информацией, рассмотрен с иной точки зрения или же более детально. В нём рассматриваются проблемы практической реализации требований, сформулированных в ряде других документов, к числу которых относятся ИСО/ТО 15801, ИСО 15489-1, MoReq2, в котором перечислены функциональные требования к организации и управлению жизненным циклом информации, сохраняемой в качестве доказательств и для сведения, и ИСО 14721, в котором описаны характеристики открытой системы для обеспечения долговременной сохранности электронных данных.

Приложения А, В и С являются справочными и дополнительными.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Управление электронными документами

**ПРОЕКТИРОВАНИЕ И ЭКСПЛУАТАЦИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ
ДЛЯ ОБЕСПЕЧЕНИЯ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ
ЭЛЕКТРОННЫХ ДОКУМЕНТОВ**

Технические требования

Electronic document management
Design and operation of an information system for the preservation
of electronic documents - Specifications

Дата введения –

1 Область применения

Настоящий стандарт содержит набор технических требований и организационных мер, которые следует реализовать в отношении захвата, хранения и доступа к электронным документам. Тем самым обеспечивается читаемость, целостность и прослеживаемость документов в течение всего срока их хранения.

Данный стандарт применим к электронным документам, которые:

- получены в результате оцифровки оригинальных бумажных документов или документов на микроформах;
- получены в результате преобразования аналогового аудио- или видеоконтента;
- изначально созданы в электронном виде в рамках электронных процессов;
- получены из других источников электронного контента, такого, как двух- или трехмерные карты, рисунки или чертежи, электронные аудио- и видеоматериалы и электронные медицинские изображения.

Данный стандарт неприменим в отношении информационных систем, в которых пользователи имеют возможность заменять или изменять документы после их ввода в систему.

Данный стандарт предназначен для следующих пользователей:

а) Организации, внедряющие информационные системы, в которых:

1) созданные путем сканирования/оцифровки электронные документы хранятся в условиях, обеспечивающих их долговременную сохранность, целостность и аутентичность по отношению к оригиналам;

2) изначально-электронные документы хранятся в условиях, обеспечивающих целостность информационного контента и читаемость документов;

3) обеспечивается прослеживаемость всех операций, связанных с электронными документами.

б) Организации-поставщики ИТ-услуг и разработчики программного обеспечения, стремящиеся создать информационные системы, обеспечивающие целостность и аутентичность электронных документов.

с) Организации-поставщики услуг доверенной третьей стороны по хранению документов.

2 Нормативные ссылки

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

ISO 2859 Sampling procedures for inspection by attributes (все части)

ISO 8601 Data elements and interchange formats — Information interchange — Representation of dates and times

ISO/TR 12033 Document management — Electronic imaging — Guidance for the selection of document image compression methods

ISO 12653-1 Electronic imaging — Test target for the black-and-white scanning of office documents — Part 1: Characteristics

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

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов (и классификаторов) на территории государства по соответствующему указателю стандартов (и классификаторов), составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины и определения, данные в ИСО 12653-1 и ИСО 12653-2, а также приведенные ниже термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для применения в сфере стандартизации, расположенные по следующим адресам:

- база МЭК «Electropedia»: доступна по адресу <http://www.electropedia.org/>;
- база ИСО «Online browsing platform»: доступна по адресу <http://www.iso.org.obp>.

3.1 доступ (access): Процессы извлечения и отображения (воспроизведения) электронных документов для использования в оперативной деятельности, в качестве доказательств или в исторических целях.

3.2 документальный фонд, документация (archive): Совокупность документов, созданных или полученных физическим или юридическим лицом или же государственным или частным учреждением или службой в ходе деловой деятельности, вне зависимости от даты их создания, формата или носителя информации.

3.3 политика хранения (archival policy): Правовые, функциональные, эксплуатационные, технические требования и требования по безопасности, которым должна удовлетворять собственная или внешняя информационная система, используемая для хранения документов.

Примечание – В приложениях А и В описаны принципы разработки политики хранения и декларации практики хранения документов.

3.4 журнал аудита жизненного цикла документального фонда (archive lifecycle log): Журнал аудита, протоколирующий все транзакции, имевшие место между передающей документы на хранение стороной и системой хранения.

3.5 реституция документального фонда (archive restitution): Совокупность процессов и методов, позволяющих отобрать и вернуть электронные документы создавшим их организациям или уполномоченным ими сторонам, а также необратимо уничтожить эти документы в системе хранения.

3.6 профиль хранения (archival system profile): Совокупность правил, которые применяются в отношении хранимых в системе дел и/или документов, имеющих общие характеристики в плане конфиденциальности, сроков хранения и действий по их истечении, а также прав доступа (например, на создание, чтение, модификацию, удаление).

3.7 устройство создания электронных свидетельств (attestation creation unit, ACU): Аппаратное и/или программное устройство формирования электронных свидетельств.

Примечание – В свидетельстве указывается идентификатор устройства и идентификатор архивно-документационной службы организации, учреждения либо третьей стороны – поставщика услуг хранения.

3.8 аудиовизуальный (audiovisual): Категория методов передачи информации преимущественно в виде сочетания звука и изображения.

3.9 контрольная информация (audit trail): Совокупность информации, необходимой для документирования истории всех существенных событий, связанных с хранимой информацией и информационной системой.

3.10 данные (data): Представление информации в формализованном виде, пригодном для передачи, интерпретации или обработки.

3.11 отметка даты и времени (date and time stamp): Последовательность символов, обозначающая дату и/или время, когда произошло определенное событие

3.12 партия документов (deposit): набор передаваемых на хранение документов, имеющих один и тот же профиль хранения.

3.13 электронная архивация, обеспечение сохранности электронных документов (digital archival): Совокупность действий, направленных на выявление, захват, классификацию, сохранение, извлечение, отображение, предоставление доступа и реституцию электронных документов, в течение сроков, необходимых для исполнения требований законодательства и удовлетворения потребностей в информации, и/или в целях сохранения культурно-исторической памяти.

3.14 электронный документ (digital document): Документ, контент которого представлен и управляется в электронной форме.

Примечание – Электронный документ представляет собой взаимосвязанные контент, логическую структуру и атрибуты отображения, которые могут быть извлечены и обработаны устройством, способным отобразить его в виде воспринимаемого человеком (или машиночитаемого) объекта. Электронный документ может быть изначально создан в электронном виде либо получен в результате преобразования аналогового документа.

3.15 хеш, дайджест, цифровой отпечаток документа (digital fingerprint): Сформированная на основе электронного документа с использованием хеш-функции последовательность битов, которая однозначно этот документ идентифицирует.

Примечание – Любая модификация электронного документа приведет к изменению значения его хеша.

3.16 электронная печать (digital seal): Способ обеспечения целостности документа посредством использования хеш-функций, электронных цифровых подписей и, опционально, отметок времени.

3.17 электронная цифровая подпись (digital signature): Данные, которые, будучи присоединёнными к электронному документу, дают возможность пользователю документа аутентифицировать его происхождение и установить его целостность.

3.18 оцифровка (digitization): Преобразование аналогового документа (зафиксированного на бумаге, микроформе, пленке, на аналоговых аудио- или видеолентах) в электронный цифровой формат с целью обработки и/или обеспечения сохранности.

3.19 оцифрованный документ (digitized document): Результат оцифровки информации, первоначально сохраненной на аналоговом носителе (на бумаге, микроформе, пленке, на аналоговой аудио- или видеоленте и т.п.).

3.20 аутентичность документа исходному (document fidelity): Свойство сохраненного документа воспроизводить всю информацию, содержащуюся в исходном оригинальном документе, которая необходима для его использования в тех же целях, для которых предназначался оригинальный документ.

Примечание – Данное понятие используется в случаях, когда имеет место какое-либо изменение формы, включая проведение оцифровки или конверсии в иной формат.

3.21 долговечность (durability): Свойство документа оставаться читаемым на протяжении всего своего жизненного цикла.

3.22 система хранения электронных документов, СХЭД (electronic information system): Система, предназначенная для приема, обеспечения долговременной сохранности, доступа и реституции электронных документов.

3.23 электронное свидетельство (electronic attestation): Информация, созданная с целью засвидетельствовать, что определенное действие или электронная транзакция имели место.

3.24 журнал событий (events log): Журнал, в котором документируется контрольная информация, относящаяся к функционированию системы,

за исключением тех операций, которые протоколируются в журнале аудита жизненного цикла документального фонда.

3.25 конверсия формата (format conversion): Операция преобразования электронного документа в другой электронный формат.

Примечание – Данная операция должна проводиться таким образом, чтобы обеспечить аутентичность полученного документа исходному.

3.26 хеш-функция (hash function): Математический алгоритм, используемый для превращения некоторых видов данных (3.10) в относительно небольшое число.

3.27 целостность (integrity): Свойство быть полным и неизменным.

3.28 читаемость (legibility): Свойство документа, заключающееся в возможности получить доступ ко всей содержащейся в нём информации.

Примечание – Этому могут способствовать определенные метаданные, связанные с документом.

3.29 сжатие с потерями (lossy compression): Алгоритм сжатия данных, при использовании которого происходит определенная потеря первоначальной информации.

Примечание – При использовании сжатия с потерями восстановленный из сжатого состояния объект является лишь приблизительным воспроизведением оригинала.

3.30 миграция носителей информации (media migration): Процесс перемещения документов с одного носителя информации на другой, в частности, в связи решением проблемы устаревания носителей информации.

3.31 метаданные (metadata): Данные, описывающие контекст, содержание (контент), структуру документов и управление ими во времени.

3.32 репликация (replication): Процесс копирования информации между дублирующими друг друга ресурсами (например, программными или аппаратными

компонентами) с целью повышения надежности, отказоустойчивости и/или доступности.

3.33 источник точного времени (time source): Внутренний или внешний компонент информационной системы, обеспечивающий надежную и объективную, соответствующую требованиям привязку к эталонному времени.

3.34 отметка времени, штамп времени (time-stamp token): Объект данных, устанавливающий связь других данных в электронной форме с конкретным временем (которое указывается по всемирному координированному времени UTC) и создающий тем самым доказательство существования указанных данных в этот момент времени.

3.35 переносимость (transferability): Возможность извлечь аутентичные электронные документы (включая информацию, данные, объекты и все взаимосвязанные метаданные) из одной информационной системы, с тем, чтобы затем перенести их в другую информационную систему с помощью заранее определенной процедуры.

Примечание – Данный вопрос особенно важен в том случае, когда информация хранится третьей стороной - поставщиком услуг хранения.

3.36 доверенная третья сторона (trusted third-party archive service provider): Поставщик услуг хранения документов (trusted third-party archive service provider): третья сторона - физическое лицо или организация, ответственная за обеспечение долговременной сохранности документов.

4 Основные характеристики и уровни требований к информационным системам

4.1 Характеристики информационных систем

Организациям, желающим минимизировать правовые и технические риски при использовании в своей деловой деятельности электронных документов, необходимо

принять как технические, так и организационные меры для обеспечения их целостности и долговременной сохранности.

В этом контексте, система хранения электронных документов должна поддерживать соблюдение политики хранения, общие принципы которой описаны в Приложении А.

Важно понимать, что речь здесь идёт об информационных системах, которые захватывают электронные документы, подлежащие долговременному хранению и использованию. Термин «захват, ввод» (capture) понимается здесь как процесс получения и обработки информации, которая впоследствии будет управляться информационной системой. В тех случаях, когда требуется обеспечить хранение и управление аналоговыми документами в электронной форме, эти документы должны сканироваться и индексироваться до их захвата в информационную систему.

Настоящий стандарт направлен на то, чтобы в системе хранения исключить возможность несанкционированного изменения или удаления сохранённых электронных документов, равно как и возможность изменения, замены новой или удаления справочной и контрольной информации о них (как в папках файловой системы, так и в базе данных).

Должны быть внедрены процедуры и меры защиты с целью:

- а) мониторинга процесса хранения;
- б) предотвращения и выявления несанкционированных модификаций или изменений в документах и в метаданных, необходимых для их поиска и отображения;
- с) обеспечения целостности контрольной информации (включая журнал аудита жизненного цикла документального фонда и журнал событий).

Такая система хранения должна обладать следующими характеристиками:

- пригодность для обеспечения долговременной сохранности;
- целостность;
- защищённость/безопасность;
- прослеживаемость.

Данный стандарт описывает:

- требования к процедурам, связанным с обработкой, обеспечением сохранности, доступа, и с реституцией изначально-электронных и отсканированных документов; а также требования к безопасности информационных систем;
- процедуры, связанные с оцифровкой аналоговых документов;
- процедуры, связанные с захватом электронных документов, обеспечением их сохранности, с доступом и реституцией;
- процедуры, связанные с возможным уничтожением документов;
- правила в отношении процедур, касающихся операторов системы;
- свидетельства об этих операциях;
- требования к материалам, оборудованию и программному обеспечению, используемым для создания системы;
- порядок аудита систем и соответствующие процедуры;
- принципы, применимые в случае использования услуг доверенных третьих сторон – поставщиков услуг хранения;
- принципы, применимые в случае привлечения субподрядчиков.

Техническая документация на системы, выданные свидетельства, а также журналы аудита, отражающие жизненный цикл документального фонда и системные события, должны сохраняться на тех же условиях, что и сами документы.

4.2 Уровни требований

Подходы различных организаций к рискам и к требованиям к информационным системам, используемым для сохранения электронных документов, могут быть специфическими и индивидуальными.

Таблица 1 описывает уровни этих требований. В ней отражены основные характеристики и практические методы их реализации на предпочитаемом организацией уровне требований, с учетом особенностей сохраняемых документов и имеющихся потенциальных рисков.

Т а б л и ц а 1 – Требования к информационным системам

Характеристика	Максимальные требования	Дополнительные требования
Пригодность для обеспечения долговременной сохранности	Применение стандартизованных или являющихся фактическими отраслевыми стандартами свободно используемых форматов	Конверсия формата Оцифровка документов
	Описание документов при помощи метаданных	Использование стандартизированных метаданных
	Миграция носителей информации	—
	Конверсия формата	Контроль и конверсия форматов в момент ввода/захвата Отслеживание и извещение об устаревании форматов Плановое, прослеживаемое выполнение конверсии форматов
	Управление изменениями в системе	—

Продолжение таблицы 1

Характеристика	Максимальные требования	Дополнительные требования
Целостность	Обеспечивается путем хранения на носителях следующих видов: – физические WORM-носители однократной записи – логические WORM-устройства на несъемных носителях, поддерживающие: – журнал событий – методы и процедуры для обнаружения и предотвращения замены записей – логические WORM-устройства на съёмных носителях (см. перезаписываемые/стираемые носители информации) – перезаписываемые/стираемые носители (обычный уровень безопасности)	Высокий уровень безопасности Усиленный уровень безопасности Высокий уровень безопасности Усиленный уровень безопасности
	Процесс ввода/захвата документов	—

Продолжение таблицы 1

Характеристика	Максимальные требования	Дополнительные требования
Целостность	Предупреждение перед выполнением уничтожения документов	—
	Описание процесса уничтожения документов	Описание порядка изменения сроков хранения Сохранение после уничтожения метаданных и контрольной информации
Безопасность	Идентификация лиц и процессов, имеющих доступ к документам	Строгая аутентификация
	Резервные копии хранимых документов	Использование носителей разного типа и формата Защита от рисков возможного затопления, пожара и т.д.
	Контролируемое использование хранимых документов (идентификация и прослеживаемость)	Строгая аутентификация Доступ в форматах, отличающихся от формата при вводе
	Непрерывная доступность документов	—
Прослеживаемость	Отметка времени и даты	Использование отметок времени от доверенной третьей стороны

Окончание таблицы 1

Характеристика	Максимальные требования	Дополнительные требования
Прослеживаемость	Ведение нормативно-методической и технической документации на систему (политика хранения, условия обслуживания, процедуры эксплуатации, жизненный цикл документов)	Адаптация к процессам организации-клиента и формирование соответствующих свидетельств
	Ведение журнала аудита жизненного цикла документального фонда и журнала событий	Подписание электронных свидетельств операций и событий (индивидуально или партиями) электронной цифровой подписью и проставление отметки времени Определение гранулярности подписываемых электронной цифровой подписью партий свидетельств о событиях Частота сохранения контрольной информации (журналов аудита)

Дополнительные требования могут быть выбраны на основе специфических потребностей организации и приемлемых уровней риска.

Соответствие информационной системы настоящему стандарту должно оцениваться с учётом выбранного организацией уровня требований.

5 Общие требования

5.1 Общие положения

Проектное решение и порядок использования информационной системы должны поддерживать внедрение процедур, обеспечивающих выполнение требований, выбранных согласно 4.2.

5.2 Техническое описание

Необходимо завести и хранить дело, содержащее техническое описание информационной системы, которое, как минимум, должно включать:

а) перечень аппаратных компонентов информационной системы с указанием присвоенных им изготовителями серийных номеров, основных характеристики этих компонентов, дат изготовления, стандартов безопасности, которым они соответствуют;

б) для сетевой системы, описание её типологии и топографии, а также описание соединительного оборудования и оборудования для обеспечения безопасности;

с) модель архитектуры данных информационных объектов и их взаимосвязей, с учетом их использования в интересах общих целей информационной системы;

д) перечень программных продуктов и сопровождающей их документации, сведения об установленных версиях и о датах их установки;

е) перечень заказных программных приложений вместе с их проектно-архитектурной документацией и с исходным кодом либо свидетельством о передаче на депозитарное хранение;

ф) описание взаимодействия между различными компонентами информационной системы;

г) описание условий физической среды (температура, минимальная и максимальная влажность и т.д.), которые производители оборудования требуют выдерживать с целью обеспечения его надлежащего функционирования и обеспечения сохранности носителей информации;

h) описание технических и физических мер и средств, позволяющих обеспечить надёжное функционирование информационных систем (например, тип источника электропитания, электрогенератор, система обнаружения пожара, избыточность/резервирование в системе и т.д.);

i) описание мер физической защиты для обеспечения безопасности (охрана, дистанционное обнаружение, сейфы, замки, электромагнитная защита и т.д.);

j) описание требований к техническому обслуживанию информационной системы.

5.3 Профили хранения

Профиль хранения представляет собой совокупность правил, которые применяются в отношении хранимых в системе документов, имеющих общие характеристики в плане конфиденциальности, сроков хранения и действий по их истечении, а также прав доступа (например, на создание, чтение, модификацию, удаление). Эти правила также определяют метаданные, которые должны быть связаны с документами, управляемыми в соответствии с назначенным им профилем.

Профиль хранения должен, в частности, устанавливать права лиц и/или приложений, авторизованных:

- a) модифицировать профиль хранения;
- b) передавать на хранение партию документов;
- c) получать доступ (просматривать или воспроизводить) документы из партии;
- d) продлевать или сокращать сроки хранения партии документов;
- e) уничтожать партию документов в плановом или внеплановом порядке.

Все действия по созданию, изменению или удалению профилей хранения должны быть задокументированы в журнале аудита жизненного цикла документального фонда, ответственность за сохранность которого несёт архивно-документационная служба организации или доверенная третья сторона – поставщик услуг хранения.

Профиль хранения может быть также определен индивидуально для отдельных электронных документов, однако такой подход может оказаться чрезвычайно

трудоемким в случае хранения больших объёмов документации. В подобных случаях предпочтительнее использовать более общие предустановленные профили хранения.

5.4 Процедуры оперативного использования

5.4.1 Общие положения

Организация должна установить процедуры захвата, хранения, предоставления доступа и реституции документов. Эти процедуры должны быть детализированы в техническом описании. Должны быть приведены, как минимум, следующие сведения:

- методы и процедуры, используемые для поиска и печати;
- методы и процедуры формирования всех видов электронных свидетельств;
- методы и процедуры хранения и обеспечения долговременной сохранности носителей информации и инфраструктур хранения;
- используемые файловые форматы;
- методы и процедуры дублирования и репликации документов и резервных копий;
- методы и процедуры, используемые для шифрования и обеспечения целостности данных.

5.4.2 Оцифрованные документы

В случае оцифровки документов, в дополнение к процедурам, описанным в 5.4.1, в техническое описание должны быть включены следующие процедуры:

- методы и процедуры, используемые для оцифровки (описание подлежащих оцифровке документов с указанием всех их специфических особенностей; необходимые предварительные операции, такие, как выбор выходных форматов, разрешения изображения, метода сжатия (в случае его использования), действия по возврату документов после оцифровки в исходное состояние (где это применимо) и т.д.);

- методы и процедуры, используемые для индексации (указатели местоположения документов, регистрационные номера документов, оборудования и сопроводительных описей, идентификаторы электронных сообщений);
- методы и процедуры, связанные с заполнением соответствующих метаданных и их возможным обогащением;
- методы и процедуры, используемые для контроля качества (использование тестовых мишеней при оцифровке, контроль числа страниц в партиях оцифрованных документов, фильтрация электронных сообщений, контроль кодов, если таковые используются, по соответствующим справочникам и т.п.);
- методы и процедуры, используемые для уничтожения исходных документов после оцифровки, где это применимо.

5.4.3 Изначально-электронные документы

Для изначально-электронных документов в дополнение к процедурам, описанным в 5.4.1, в техническое описание должны быть включены следующие процедуры:

- методы или процедуры, используемые для передачи, получения и управления подлежащими сохранению документами;
- методы и процедуры, связанные с заполнением соответствующих метаданных и их возможным обогащением;
- методы и процедуры, касающиеся преобразования форматов электронных документов во время их ввода в систему хранения или же впоследствии, в случае устаревания форматов.

5.5 Безопасность

5.5.1 Организация и управление безопасностью

В каждой организации должна быть внедрена процедура менеджмента для обеспечения безопасности системы хранения электронных документов (СХЭД).

Ответственность за обеспечение безопасности СХЭД должна быть возложена на конкретное структурное подразделение.

В части требований к безопасности следует обращаться к стандарту ГОСТ Р ИСО/МЭК 27001 и взаимосвязанным с ним стандартам.

Отвечающее за безопасность структурное подразделение должно быть отдельным от подразделений, ответственных за эксплуатацию информационных и телекоммуникационных систем. Структура и порядок управления данным подразделением должны быть четко определены и известны всему персоналу организации.

При организации и управлении безопасностью СХЭД должны применяться принципы, унаследованные от общей стратегии или политики организации в области безопасности, а также уже существующие правила, в том числе по следующим вопросам:

- управление ключами от помещений;
- системы безопасности для детектирования, обнаружения вторжений и сигнализации;
- соответствие оборудования нормам безопасности труда (см. стандарт МЭК 61000-4);
- использование программного обеспечения, для которого можно получить исходные коды;
- разработка адекватно документированного и протестированного заказного программного обеспечения;
- управление профилями доступа к информационной системе (директория);
- использование сетей передачи данных, имеющих функциональные возможности для контроля целостности;
- назначение лиц, ответственных за безопасность;
- использование услуг сторонних поставщиков (безопасность, охрана, уборка, техническое обслуживание).

5.5.2 Оценка риска

Меры безопасности часто разрабатываются несистематически, в качестве реакции на инциденты безопасности или же в зависимости от наличия программных средств. При использовании подобного подхода в системе безопасности часто возникают бреши, которые закрываются лишь впоследствии. Более структурированный подход заключается в анализе информационных активов организации и определении факторов риска (исходя из ценности активов, уязвимости системы и вероятности атаки). Затем может быть разработана и утверждена политика информационной безопасности, на соответствие которой может быть проведен аудит мер безопасности.

Организация должна провести анализ рисков информационной безопасности и задокументировать полученные результаты.

Особое значение имеют меры безопасности, реализованные для контроля и управления как регулярно используемыми, так и резервными носителями информации. Анализ риска должен охватывать факторы риска и уязвимости, соответствующие типу используемых носителей (это, например, могут быть WORM-носители однократной записи или перезаписываемые носители).

В случае использования носителей информации различных типов, следует проанализировать влияние этого фактора на результаты анализа рисков.

По завершении анализа риска, по его результатам должны быть предприняты соответствующие действия в рамках пересмотра и актуализации реализованных мер безопасности. В процессе пересмотра учитываются такие факторы, как баланс между затратами на внедрение, достигнутым уровнем безопасности и оценкой рисков.

Исходя из результатов анализа рисков, следует заново оценить эффективность существующих мер безопасности.

Там, где такая оценка указывает на уместность внесения изменений в процедуры безопасности, соответствующие изменения должны быть реализованы.

5.5.3 Физическая безопасность

Необходимо принять меры для обеспечения физической безопасности, включая предотвращение несанкционированного доступа к оборудованию, к телекоммуникационным системам и к носителям информации - в особенности к тем ним, на которых хранятся электронные документы, поддерживающая доступ к ним информация, журналы аудита и резервные копии.

Для минимизации риска рекомендуется использовать несколько защищенных зданий/помещений для хранения в удаленных друг от друга местах носителей или систем, содержащих резервные копии (экземпляры) информации (а также, если требуется обеспечить непрерывность доступа, то и поддерживающего работу с ними оборудования).

Съемные носители должны постоянно контролироваться во время их обработки и/или передачи из одной защищенной зоны в другую. Должна иметься возможность на любой заданный момент времени установить всех держателей носителей информации.

Вне периодов их реального использования съемные носители должны храниться в специально выделенных защищенных зонах.

Если предполагается проводить уничтожение документов, то должны быть реализованы соответствующие процедуры обеспечения безопасности этих операций, как для аналоговых, так и для электронных документов.

В случаях, когда необходимо уничтожить содержащие документы носители информации, следует предпринять соответствующие меры для обеспечения невозможности восстановления ранее записанной на носителях информации.

5.5.4 Безопасность оборудования

Меры безопасности, относящиеся к оборудованию и программному обеспечению, по отдельности или совместно способствуют обеспечению безопасности информационных систем, поддерживая:

а) идентификацию аппаратных конфигураций, включая периферийные устройства;

b) меры контроля и управления, обеспечивающие отсутствие злонамеренных или случайных модификаций аппаратных конфигураций;

c) меры контроля и управления, обеспечивающие, что только авторизованные пользователи могут получить доступ к оборудованию.

Соответственно, вопросы безопасности должны приниматься во внимание при выборе оборудования и в ходе его установки и эксплуатации.

Чтобы ограничить риски незаконного перехвата информации третьими сторонами вследствие побочных электромагнитных излучений, рекомендуется тестировать оборудование на соответствие требованиям стандарта МЭК 61000-4 (все части).

5.5.5 Безопасность программных продуктов и заказного программного обеспечения

Программные продукты и заказное программное обеспечение являются неотъемлемой частью конфигурации системы; соответственно, они должны подчиняться тем же правилам безопасности, что и оборудование.

Выбирая операционные системы и программные продукты, следует отдавать предпочтение тем из них, которые предоставляют:

- средства контроля доступа, обеспечивающие усиленную защиту;
- защиту от вторжений и от вредоносного программного обеспечения;
- средства контроля и управления, исключающие внесение случайных или злонамеренных изменений в конфигурации программного обеспечения.

Безопасность программного обеспечения должна достигаться с использованием:

- средств контроля доступа, обеспечивающих, что только авторизованные пользователи и только в соответствии со своими правами доступа могут использовать программное обеспечение и информацию;
- систем обнаружения и мониторинга, позволяющих выявлять любые попытки несанкционированного доступа и оповещать о них.

Рекомендуется использовать программное обеспечение, которое находится в публичном доступе; или же, когда это возможно, получать от поставщика его исходные коды.

При разработке программного обеспечения должны использоваться строгие методики, ответственность за выбор и контроль над надлежащим применением которых несет лицо, ответственное за программное приложение.

Перед вводом в эксплуатацию, программные продукты и заказное программное обеспечение должны быть надлежащим образом протестированы в вычислительной системе, отличной от основной производственной вычислительной системы, либо в производственной вычислительной системе в периоды, когда не ведётся оперативная деятельность. При этом предварительно должны быть сделаны резервные копии данных и индексов и отсоединены все соответствующие съёмные носители информации в системе.

Вопросы безопасности доступа и предоставления прав доступа к системе хранения электронных документов должны быть тщательно изучены, а соответствующие меры должны разрабатываться и реализовываться с самого начала проектирования системы.

Программные продукты и заказное программное обеспечение должны быть особо защищены, и права доступа, разрешающие их изменение или модификацию, должны предоставляться только авторизованным лицам.

О сбоях и отказах следует немедленно известить службу безопасности, а неисправная часть информационной системы должна быть как можно скорее изолирована.

5.5.6 Техническое обслуживание информационной системы

В техническое описание системы должны быть включены сведения, описывающие каждую из операций технического обслуживания. Должны быть, в том числе, указаны характер операции технического обслуживания - профилактическая либо ремонтно-восстановительная; и кому доверяется её выполнение - самой организации либо специализированному внешнему поставщику услуг.

Съемные носители, содержащие электронные документы и взаимосвязанные с ними метаданные, никогда не должны оставаться в приводах во время операций технического обслуживания.

Если носители являются несъемными, то перед любой операцией технического обслуживания создается работоспособная резервная копия (см. 5.5.8).

Любое тестирование должно проводиться с использованием специально предназначенных для этой цели съемных носителей. Если носители являются несъемными, то следует исключить возможность изменения или уничтожения записанной на них информации в ходе тестирования.

Для обеспечения надлежащего функционирования информационной системы должно выполняться профилактическое техническое обслуживание. Следует, в частности, проводить регулярные проверки несъемных носителей и приводов для съемных носителей с целью убедиться, что они находятся в надлежащем рабочем состоянии и используются в соответствии с рекомендациями изготовителей.

5.5.7 Управление изменениями в системе и миграция носителей информации

Периодически выполняемые операции по обновлению и модификации либо замене оборудования или программного обеспечения должны заранее планироваться.

Все операции такого рода должны быть подробно описаны в техническом описании информационной системы, и их выполнение должно протоколироваться в журналах аудита.

При выполнении периодических операций обновления должны быть обеспечены долговременная сохранность и целостность документов и их метаданных.

Могут сложиться две следующие ситуации:

а) новая система способна читать носители информации, использовавшиеся в старой системе. В этом случае, прежде чем приступить к выводу из эксплуатации старой системы, следует убедиться, что все носители информации хорошо читаются на новом оборудовании.

b) новая система не в состоянии читать носители информации, использовавшиеся в старой системе. В таком случае следует скопировать всю совокупность содержащихся на старых носителях документов на новые носители с использованием программно-аппаратной конфигурации, которая временно включает в себя два поколения системы.

5.5.8 Резервные копии

Система хранения электронных документов должна быть спроектирована и внедрена таким образом, чтобы всегда имелись по крайней мере два экземпляра одного и того же документального фонда, хранящиеся в географически удаленных друг от друга местах. Желательно, чтобы по крайней мере один из таких экземпляров был записан на непerezаписываемых носителях информации.

Используемые для резервных копий носители информации могут по своей природе и типу отличаться от первичных носителей информации.

В случае использования несъемных носителей информации необходимо установить две информационные системы в географически удаленных друг от друга местах.

В случае использования съемных носителей информации, запись документов на резервный носитель должна производиться как можно скорее, с тем, чтобы быстрее поместить их резервные копии на хранение в место, географически удаленное от исходной системы.

Каждый раз, когда создается резервная копия, сведения о процессе её создания, а также имена и характеристики сохраненных файлов должны быть зафиксированы в журнале событий.

5.5.9 Непрерывность доступа к документам

Как и для любой другой информационной системы, должна быть предусмотрена документированная процедура восстановления СХЭД после инцидентов и катастроф (также известная как план обеспечения непрерывности деловой деятельности).

Эта процедура должна обеспечивать восстановление системы без какой-либо утраты данных, метаданных, журналов аудита и любых иных наборов данных (списка пользователей, профилей хранения и т.д.).

Программное обеспечение и процедуры восстановления данных системы должны быть задокументированы в техническом описании.

Информационная система должна быть спроектирована и реализована таким образом, чтобы в любой заданный момент времени ни один документ, принятие которого на хранение подтверждено системой, не мог быть потерян.

Информационная система должна автоматически документировать все процессы восстановления.

5.6 Проставление отметок даты и времени

Данный стандарт допускает два варианта проставления отметок даты и времени, в зависимости от того, кто их формирует - внутренняя служба времени или служба времени доверенной третьей стороны. Отметки даты и времени должны, как минимум, обладать следующими свойствами:

- a) отметки времени соответствуют действующим стандартам;
- b) обеспечивается хранение отметок времени в течение установленных сроков;
- c) имеется источник эталонного времени;
- d) отметки времени формируются в соответствии с контролируемой политикой создания и использования отметок даты и времени.

Для операций, связанных с проставлением отметок времени и даты, в техническом описании должен быть указан выбранный способ формирования этих отметок.

Форматы даты и времени должны соответствовать стандарту ГОСТ Р 7.0.64-2018.

Отметка даты и времени должна включать полное представление календарной даты и времени дня с указанием часов, минут, секунд и десятичных долей секунд, представленные в следующем формате:

YYYY-MM-DDThh:mm:ss,sTZD

где:

YYYY год, записанный 4 цифрами;

MM месяц, записанный 2 цифрами (от 01 до 12, где 01 - январь);

DD день месяца, записанный 2 цифрами (от 01 до 31);

hh час, записанный 2 цифрами (от 00 до 24);

mm минуты, записанные 2 цифрами (от 00 до 59);

ss секунды, записанные 2 цифрами (от 00 до 60);

s десятичная часть секунды, записанная одной или несколькими цифрами;

TZD указание на часовой пояс (Z при использовании Всемирного времени, либо в формате +hh:mm или -hh:mm).

Пример – 2007-08-29T09:36:30,45+02:00.

Чтобы выбрать нужный уровень точности измерения времени, важно определить максимально возможную частоту возникновения событий в системе и затем выбрать достаточно высокую точность отсчета времени, обеспечивающую, что два таких события не могут иметь одну и ту же дату и время.

При указании сведений о дате следует использовать Всемирное координированное время (Coordinated Universal Time, UTC).

В техническом описании следует описать источники времени и методы корректировки и контроля над ними, а также процессы синхронизации часов различных компонентов системы.

Если для системы хранения электронных документов нужны отметки даты и времени, они должны формироваться устройством создания электронных свидетельств или же независимой доверенной третьей стороной, внешней по отношению к системе хранения электронных документов.

5.7 Контрольная информация

5.7.1 Общие положения

Все события, связанные с функционированием информационной системы или с жизненным циклом документов, должны документироваться/протоколироваться. Информационная система должна автоматически создавать и вести журналы аудита (логи), снабжая записи в них отметками даты и времени (см. 5.6). События должны последовательно и полно документироваться в соответствующих журналах аудита.

Все журналы аудита и порядок их функционирования должны быть описаны в техническом описании системы. Должна быть обеспечена легкодоступность содержащейся в журналах аудита информации.

Резервное копирование журналов аудита должно проводиться с периодичностью и на условиях, установленных политикой хранения, на носителях информации, обеспечивающих как минимум ту же долговечность и целостность, что и для документов, к которым эти журналы аудита относятся.

Журналы событий должны быть недоступны для обычных пользователей и операторов; администрирование журналов аудита должен осуществлять только специально авторизованный оператор (системный администратор).

Журналы аудита служат основой для формирования электронных свидетельств. Электронные свидетельства должны сохраняться в том же порядке, что и документы, к которым они относятся.

5.7.2 Защищённое хранение контрольной информации

Независимо от того, какой тип носителей используется для хранения контрольной информации, должна иметься возможность доказать непрерывность протоколирования событий в информационной системе в журналах аудита.

Журналы аудита должны храниться в столь же защищённых условиях, что и документы.

5.7.3 Журнал аудита жизненного цикла документального фонда

Журнал аудита жизненного цикла документального фонда может быть общим или же вестись отдельно для каждой организации-владельца документов.

Журнал аудита жизненного цикла должен включать следующие электронные свидетельства:

- а) свидетельство о первоначальной передаче на хранение партии документов;
- б) свидетельства об изменениях срока хранения партии документов, если таковые имели место;
- в) свидетельство об уничтожении по истечении срока хранения либо о досрочном уничтожении партии документов, где это уместно;
- г) свидетельство о реституции партии документов, где это уместно;
- д) свидетельства о всех операциях создания, изменения или удаления профиля хранения.

Журнал аудита жизненного цикла документального фонда должен обновляться в момент протоколирования операций создания, изменения или удаления профиля хранения и в момент формирования нового электронного свидетельства.

Возможность полного или частичного просмотра журнала аудита жизненного цикла документального фонда должен иметь любой пользователь, авторизованный на это в соответствии с профилем хранения.

Архивно-документационная служба организации либо третьей стороны – поставщика услуг хранения должна предоставить всем лицам, авторизованным в соответствии с профилем хранения на выполнение такой операции, средства, позволяющие им проверить целостность и происхождение всего журнала аудита жизненного цикла документального фонда или любой его части.

После каждого обновления архивно-документационная служба организации или учреждения либо третьей стороны – поставщика услуг хранения должна предоставлять данные, позволяющие авторизованным лицам проверять целостность всего этого журнала аудита или любой его части.

5.7.4 Журнал событий

Журнал событий должен быть в информационной системе один. Он должен фиксировать, кто использовал систему (будь то пользователь-человек или автоматическая система), когда она была использована, что было сделано в информационной системе и каковы были результаты. Журнал событий должен отслеживать, кто получал доступ к информационной системе, соблюдали ли сотрудники установленные процедуры и не были ли какие-либо действия аварийными, мошенническими, злонамеренными или несанкционированными.

Журнал событий должен содержать три раздела:

- a) раздел для всех событий, связанных с хранением документов;
- b) раздел для всех событий, связанных с безопасностью;
- c) раздел для всех событий, связанных с информационной системой.

Основная функция журнала событий - осуществление внутреннего контроля. Он должен давать возможность анализировать всю информацию, сообщения об ошибках и иные предупреждения, формируемые во время эксплуатации информационной системы, такие, как сообщения о неудачном либо удачном выполнении операций.

В информационных системах, использующих физические или логические WORM-носители однократной записи, в журнале событий должны фиксироваться подключение и отключение каждого носителя информации. В журнале событий должны быть отражены операции по копированию содержимого одного носителя на другой.

Сведения в журнале событий должны обеспечить доказательства того, что соблюдались установленные процедуры, и должны включать, по крайней мере, следующую информацию о каждом значимом событии:

- дата и время операции, указанные в соответствии со стандартом ИСО 8601;
- выполненная операция;
- идентификация использованных технических компонентов;
- название соответствующего процесса и его версия;
- идентификация оператора, где это уместно.

6 Носители информации

6.1 Характеристики носителей информации

Определения различных типов носителей информации приведены в таблице 2.

Т а б л и ц а 2 – Определение типов носителей информации

Тип носителя	Определение
Съемные носители информации	Физические носители информации, которые могут быть извлечены из устройств чтения-записи (приводов); либо устройства хранения данных, которые могут быть легко извлечены из системы, специально для этого спроектированы и не являются интегральной частью инфраструктуры системы. Могут использоваться оптические или магнитные технологии, запись может осуществляться на дисках, лентах, портативных жёстких дисках и твердотельных накопителях.
Несъемные носители информации	Устройства хранения и чтения/записи данных, которые не предназначены для извлечения из системы во время её нормальной работы, а также физические носители информации, которые являются неотъемлемой частью таких устройств и не могут быть из них извлечены. Обычно представляют собой магнитные жёсткие диски или твердотельные накопители.
Физические WORM-носители	Информация записывается однократно с использованием процесса, необратимым образом физически модифицирующего носитель информации.

Окончание таблицы 2

Тип носителя	Определение
	После такой модификации информация уже не может быть изменена или удалена.
Логические WORM-носители	Носитель информации является перезаписываемым, однако соответствующее программное и/или аппаратное обеспечение предотвращают какое-либо изменение или удаление один раз записанной информации.
Перезаписываемые носители	Данный тип носителей позволяет записывать, модифицировать или удалять информацию без каких-либо ограничений.

В таблице 3 указаны те разделы настоящего стандарта, которые описывают порядок использования различных допустимых типов носителей информации.

Т а б л и ц а 3 – Использование различных типов носителей информации

Характеристики носителя	Тип носителя		
	Физический WORM	Логический WORM	Перезаписываемый
Съемный	Раздел 7	Разделы 7 и 8	Разделы 7 и 9
Несъемный	–	Раздел 8	Раздел 9

6.2 Обеспечение долговременной сохранности архивных носителей информации

Как съемные, так и несъемные носители информации, используемые для хранения документов (архивные носители), должны храниться в адекватных

их физическим характеристикам условиям, согласно указаниям изготовителя или соответствующих стандартов.

Состояние записанных данных должно регулярно контролироваться. Контроль и периодическая проверка носителей информации должны проводиться в рамках процесса контроля качества. Такой процесс является ключевым фактором для обеспечения долговременной сохранности записанных на носителях информации данных.

Миграция записанных данных на новый носитель должна производиться по достижении указанного изготовителем ожидаемого срока службы носителя или же тогда, когда результаты тестов носителя показывают, что его характеристики приближаются к предельно допустимым.

Обновление носителей информации должно обеспечить долговременное сохранение целостности и доступности документов.

7 Системы, использующие съемные носители

7.1 Общие положения

Как правило, система хранения электронных документов не обращается непосредственно к носителям информации. Информация фактически записывается на логические тома.

Логический том может располагаться на одном или нескольких носителях информации, а носитель может быть частью одного или нескольких логических томов. Носители информации – это реально существующие физические объекты, в то время как тома являются логическими, виртуальными сущностями.

При использовании съемных оптических носителей, структуры логических томов и файловые структуры должны соответствовать стандартам ИСО/МЭК 13490 или ИСО/МЭК 13346.

7.2 Инициализация логических томов на съёмных носителях

Поскольку технологии постоянно эволюционируют, необходимо сохранять историю аппаратных конфигураций, использовавшихся в момент записи документов.

До записи на него первого документа, логический том должен быть инициализирован с указанием следующей информации:

- а) уникальный идентификатор носителя информации;
- б) дата и время инициализации;
- с) название организации.

7.3 Заккрытие логических томов на съёмных носителях

Когда логический том заполнен, и после того, как последний документ был записан, том, по возможности, должен быть закрыт. Соответственно, вслед за последней пользовательской информацией должны быть записаны следующие сведения:

- а) дата и время закрытия тома;
- б) количество файлов, записанных на носителе информации.

Заккрытие тома должно исключить возможность дальнейшей записи на этот том.

7.4 Маркировка физических WORM-носителей информации

При использовании физических WORM-носителей однократной записи, безопасность информационной системы опирается на однозначную идентификацию носителей и на ведение журнала событий, в котором фиксируются все случаи миграции этих носителей.

Как следствие, необходимо иметь возможность индивидуально идентифицировать каждый физический WORM-носитель и реализовать методы и процедуры, позволяющие выявлять и/или предотвращать замену одного носителя на другой. Способ выполнения этих требований должен быть отражен в техническом описании.

8 Системы, использующие логические WORM-носители

Поскольку логические WORM-носители по определению являются физически перезаписываемыми, то информационные системы, использующие как несъемные, так и съемные логические WORM-носители должны рассматриваться, в контексте данной части ИСО 14641, как информационные системы, использующие перезаписываемые носители.

Кроме того, при использовании съемных логических WORM-носителей должны применяться требования раздела 7.

9 Системы, использующие перезаписываемые носители информации

9.1 Общие положения

Если система хранения электронных документов использует съемные или несъемные перезаписываемые носители, то обеспечение целостности опирается на принцип, согласно которому однажды сделанную запись должно быть невозможно изменить так, чтобы это не было замечено и зарегистрировано, за счет использования криптографических методов и формирования электронных свидетельств.

Можно выделить три уровня безопасности: стандартный, усиленный и продвинутый. Эти уровни требуют использования соответствующих криптографических методов: функций хеширования, отметок даты и времени и/или усиленных электронных подписей.

Если уровень безопасности подразумевает использование усиленной электронной подписи, то подписантом является тот, кто имеет в своем распоряжении и активирует средство создания усиленной электронной подписи. Подписантом может быть физическое лицо, юридическое лицо или процесс. В тех случаях, когда подписантом является юридическое лицо или процесс, усиленная

электронная подпись может автоматически создаваться в момент выполнения соответствующей операции.

Усиленная электронная подпись должна удовлетворять следующим требованиям:

- а) она однозначно связана с подписантом;
- б) она позволяет идентифицировать подписанта;
- с) она создается с использованием средств, которые подписант может сохранять под своим единоличным контролем;
- д) она таким образом связана с подписанными данными, что любые последующие изменения в данных могут быть обнаружены.

Примечание – Усиленная электронная подпись соответствует определению, данному Европейским институтом телекоммуникационных стандартов (European Telecommunications Standardization Institute, ETSI) в спецификациях ETSI TS 101 733 (CAAdES) и ETSI TS 101 903 (XAdES).

При использовании любого из этих трех уровней безопасности, должно формироваться и регистрироваться в журнале аудита электронное свидетельство, подтверждающее первоначальную передачу на хранение партии документов. Оно, как минимум, должно включать хеши передаваемых на хранение документов и логический адрес хранения, независящий от места (мест) хранения. Свидетельства должны служить доказательствами того, что соответствующие операции были запрошены авторизованным лицом и выполнены под полным контролем системы хранения электронных документов организации либо доверенной третьей стороны – поставщика услуг хранения.

9.2 Стандартный уровень безопасности

На данном уровне любое лицо или процесс, авторизованные в профиле хранения на выполнение операции, должны, как минимум, быть аутентифицированы с использованием идентификатора и пароля, соответствующих политике

безопасности организации или доверенной третьей стороны – поставщика услуг хранения.

Чтобы предотвратить любую модификацию записей в журнале жизненного цикла документального фонда, данный журнал не реже одного раза в день должен снабжаться отметкой даты и времени, даже если в этот день не было никакой активности. Должно быть обеспечено непрерывное ведение данного журнала аудита.

Данный уровень безопасности должен опираться на журналы аудита, которые ведутся в системе хранения электронных документов организации или доверенной третьей стороны – поставщика услуг хранения.

9.3 Усиленный уровень безопасности

На данном уровне, в дополнение к требованиям стандартного уровня (9.2), необходимо выполнить следующие дополнительные условия:

Каждое свидетельство, зафиксированное в журнале аудита жизненного цикла документального фонда, должно быть подписано усиленной электронной подписью устройством создания свидетельств системы хранения электронных документов организации или доверенной третьей стороны – поставщика услуг хранения.

Система хранения электронных документов организации либо доверенной третьей стороны – поставщика услуг хранения для каждой политики хранения должна указывать, какая политика или политики использования электронной подписи применимы в отношении свидетельств, электронно подписываемых устройством создания свидетельств.

9.4 Продвинутый уровень безопасности

На данном уровне, в дополнение к требованиям усиленного уровня (9.3), необходимо выполнить следующие дополнительные условия:

Любое лицо, авторизованное на выполнения операций в соответствии с профилем хранения, должно подписывать соответствующие распоряжения с использованием усиленной электронной подписи. Каждое электронное

свидетельство должно содержать такое подписанное распоряжение и скрепляться подписью устройства создания свидетельств, как это описано в требованиях усиленного уровня.

Архивно-документационная служба организации либо доверенной третьей стороны – поставщика услуг хранения для каждой политики хранения должна указать политику или политики использования электронной подписи, применимые к распоряжениям, которые электронным образом подписываются лицами, авторизованными в профиле хранения на выполнение операций.

10 Процессы ввода/захвата документов в систему хранения

10.1 Документы в электронном виде

10.1.1 Общие положения

Передаваемые на хранение документы в электронном виде должны храниться в стандартизованных или являющихся фактическими отраслевыми стандартами файловых форматах, спецификации которых должны быть свободно доступны в течение всего жизненного цикла документов. В политике хранения должны быть приведены ссылки на стандарты, относящиеся к различным встречающимся типам электронных документов, а также ссылки на спецификации форматов, с тем, чтобы обеспечить как возможность использования документов во времени, так и стабильность их информационного контента.

10.1.2 Процедура ввода документов в систему хранения

Процедура ввода в обязательном порядке включает две отдельные, но взаимосвязанные операции: запись файлов документов на устройства хранения и обновление каталогов с использованием ассоциированных с документами метаданных. Ввод может быть подтвержден только тогда, когда обе эти операции будут успешно завершены.

Должны быть описаны процессы контроля и записи электронных документов и ассоциированных с ними метаданных.

Электронные документы должны быть записаны на устройство хранения в виде файлов, идентифицируемых с помощью уникальных идентификаторов.

Для каждого принимаемого на хранение документа информационная система, как минимум, должна:

- а) проверить качество записи документа на устройство хранения, используя поддерживаемые применяемым оборудованием коды для обнаружения и исправления ошибок;
- б) подтвердить, что новый документ зарегистрирован в каталоге информационной системы;
- с) обеспечить связь между физическим местоположением документа и его логической идентификацией.

10.1.3 Электронные документы, структурированные с помощью языка разметки

В эту группу входят документы, состоящие из текстовых и/или нетекстовых компонентов, структурированные с помощью стандартизованного языка разметки XML. Данный тип документа может ссылаться на логическую модель, ссылка на которую дана в начале документа.

Процедура приема на хранение документов этого типа должна охватывать все составляющие его компоненты, том числе XSD-схемы, таблицы кодировок, связанные документы и т.д.

10.1.4 Электронные документы в формате представления документов

Речь идёт о формате кодирования, обеспечивающем отображение и печать документа. Для хранения должны использоваться стандартизованные или являющиеся фактическими отраслевыми стандартами файловые форматы, спецификации которых должны быть опубликованы и свободно доступны на протяжении жизненного цикла документа.

Примечание – Форматы семейства PDF/A, описанные в стандарте ИСО 19005 (все части) соответствуют настоящему требованию.

10.1.5 Другие форматы электронных документов

Если принято решение хранить электронный документ в его исходном формате, и если спецификация этого формата не являются общедоступными, то обеспечение долговременной сохранности документа в его исходном формате может потребовать сохранения соответствующих аппаратных и/или программных средств для доступа к информации.

10.1.6 Потоки печати

В настоящем подразделе рассматриваются файлы, посылаемые на высокопроизводительные принтеры. Вместе с выводимыми на печать данными эти файлы могут содержать ссылки на внешние файлы, называемые «ресурсами». В чисто таких «ресурсов» могут входить шрифты, изображения, наложения, формы и т.д. Эти «ресурсы» необходимы для отображения и воспроизведения электронного документа.

Представляющие документ файлы и все связанные с ним ресурсы, необходимые для его отображения, должны храниться в одних и тех же условиях, с тем, чтобы сохранить связи между всеми компонентами.

Для подобных «составных» документов, все внешние файлы, на которые они ссылаются должны быть представлены в стандартизованных или являющиеся фактическими отраслевыми стандартами файловых форматах. Совокупность образующих электронный документ файлов должна давать возможность аутентично воспроизвести документ без использования каких-либо специфических преобразований.

10.1.7 Проверка электронных документов

Как минимум, должны проверяться:

- а) количество и объем принятых на хранение документов;
- б) соответствие ассоциированных с документами метаданных установленным форматам;
- в) либо отсутствие кодированных данных, либо, как альтернатива, использование осмысленных значений кодов, позволяющих их интерпретировать.

Могут быть проведены дополнительные проверки на соответствие форматов передаваемых на хранение документов форматам, установленным политикой хранения.

10.1.8 Контроль целостности электронных документов, передаваемых из исходных программных приложений

Целостность документов или партий документов, полученных от внешних деловых программных приложений, должна быть проверена до их загрузки в информационную систему.

Необходимо рассмотреть два случая:

- если документы или партии документов уже содержат или ассоциированы с элементами, позволяющими провести контроль целостности (усиленные электронные подписи, электронные печати, отметки времени, хеши), то при получении партии документов информационной системой должна быть проведена проверка целостности на основе этих элементов;
- если документы или партии документов не содержат каких-либо элементов, позволяющих провести такой контроль, то следует рассмотреть вопрос об интеграции соответствующих средств.

10.1.9 Сбор/захват метаданных

Метаданные могут быть собраны несколькими, не исключаящими друг друга способами:

- а) автоматическое извлечение метаданных из документа;
- б) автоматическое извлечение метаданных из информационной системы, которая создала электронный документ;
- с) ввод или обогащение метаданных в процессе ввода/захвата документов.

Процедуры создания и контроля метаданных должны быть описаны в техническом описании.

При вводе электронных документов, метаданные должны включать следующую информацию о создании и происхождении этих документов:

- идентификация организации или подразделения, инициирующих передачу документов на хранение;
- идентификация архивно-документационной службы, принимающей документы на хранение;
- дата и время формирования или поступления партии передаваемых на хранение документов;
- метод преобразования, применяемый к оригинальным документам, если их первоначальный формат не соответствует положениям раздела 10.1.1;
- формат(ы) кодирования документов;
- срок сохранения документов и действия, выполняемые по его истечении;
- права доступа к передаваемым на хранение документам;
- объём партии документов.

10.1.10 Индексирование и поиск документов

Электронные документы должны классифицироваться, идентифицироваться и индексироваться с использованием метода, позволяющего вести поиск конкретного документа или конкретной группы документов.

Такие индексы должны быть построены на основе метаданных документов. Индексирующая информация должна сохраняться информационной системой либо в виде простого автономного индекса, относящегося только к документам; либо, в более сложных информационных системах в виде, например, составной части более обширной базы данных.

Информационная система должна быть спроектирована таким образом, чтобы непреднамеренные действия пользователя не приводили бы, без выдачи пользователю соответствующего предупреждения, к изменению или утрате индексов или связей между логическим и физическим адресами документов.

10.2 Бумажные документы и документы на микроформах

10.2.1 Средства оцифровки/сканирования документов

Устройства оцифровки/сканирования документов, первоначально созданных на бумаге или микроформах, должны быть полностью описаны, включая:

- а) допустимые физические характеристики документов, которые могут обрабатываться устройствами оцифровки;
- б) технические возможности устройств оцифровки;
- в) оптические элементы устройств оцифровки (если есть), с указанием их механизмов функционирования и настройки;
- г) механизмы настройки устройств оцифровки и их использование.

10.2.2 Средства обработки изображений

Для создания качественных электронных графических образов и/или для уменьшения размера файлов может потребоваться использование программных и/или аппаратных средств, обеспечивающих обработку этих графических образов после оцифровки. Последствия каждого из процессов обработки и их ограничения должны быть указаны в техническом описании.

Наиболее часто используются следующие методы:

- а) преобразование изображения из цветного или в градациях серого цвета в монохромное;
- б) устранение перекосов;
- в) удаление пятен/очистка фона;
- г) обрезка и очистка краёв изображения;

е) удаление наложений, логотипов, водяных знаков и иных видов ненужной информации;

ф) удаление пустых страниц.

Все эти процессы должны применяться с осторожностью, после тщательного анализа, поскольку они способны повлиять на аутентичность электронного графического образа по отношению к исходному документу. В частности, процедуры преобразования изображений в оттенках серого цвета или цветных изображений в монохромные должны быть тщательно протестированы и проверены до их реализации на практике.

Процесс удаления пятен может привести к удалению из изображения определенных элементов информации, таких как запятая, надстрочный знак или мелкий элемент диаграммы, поэтому данный процесс должен быть протестирован перед его использованием. Результаты тестирования должны быть сохранены в составе технического описания.

Программное обеспечение, применяемое для «снятия» типовых форм/фонового изображения (removal of overlays) и сохраняющее только переменное содержание, может использоваться при условии, что задействованные в информационной системе соответствующие функциональные возможности полностью отражены в техническом описании. Помимо этого, когда для точного воспроизведения документа требуется воссоздать его путем слияния переменного содержания и формы, то используемая при этом версия формы должна быть идентична форме, снятой в процессе оцифровки и обработки страницы.

В техническом описании должно быть отражено управление версиями форм/фонового изображения и логической связью между переменным контентом документа и соответствующей версией формы.

Формы/фоновые изображения рассматриваются как элементы документа и поэтому должны сохраняться в том же порядке, что и другие элементы документа.

В тех случаях, когда требуется сохранить информацию во всей её полноте, такие методы использовать не рекомендуется. В остальных случаях в техническом описании необходимо указать причины использования этих методов.

С автоматическим удалением пустых страниц связан потенциальный риск потери информации. В случае реализации такого метода рекомендуется убедиться,

что применяемый метод является надежным и не удаляет содержащую информацию страницы. В техническом описании должны быть отражены процедуры, используемые для обеспечения надежности этой операции. В частности, целесообразно использовать механизмы, обеспечивающие подсчет числа удаленных страниц в сопоставлении с числом сохраненных страниц.

Использование стандартных тестовых мишеней (см. стандарты ИСО 12653-1 и ИСО 12653-2) позволяет объективно оценить и откалибровать систему и определить влияние программного обеспечения для обработки изображений.

10.2.3 Процедура захвата бумажных документов и документов на микроформах

10.2.3.1 Общие положения

По завершении процесса захвата бумажных документов или документов на микроформах, оператор должен сформировать свидетельство о проведении оцифровки, в котором, как минимум, должны быть указаны имя оператора, дата проведения оцифровки/сканирования, время начала и окончания сканирования, идентификаторы первого и последнего оцифрованных документов и количество отсканированных страниц.

После проверки отсканированных изображений, владелец документов или его уполномоченный представитель должен сформировать свидетельство (акт) об их приёмке. Если свидетельство относится к партии документов, то в нём должно быть указано количество графических образов и документов.

10.2.3.2 Подготовка бумажных документов

Организация должна обеспечить, чтобы качество создаваемых ею бумажных документов, соответствовало применяемым методам оцифровки и/или записи на микроформы. Как созданные организацией, так и полученные из внешних источников порванные или мятые документы могут потребовать проведения дополнительных подготовительных работ перед оцифровкой/записью

на микроформы, однако при этом текст документов не должен ни модифицироваться, ни ретушироваться с целью улучшения читаемости, поскольку это может негативно повлиять на аутентичность электронных документов или записанных на микроформы образов в сопоставлении с исходными документами.

По мере возможности, при создании и обработке документов, которые предполагается оцифровать, должны использоваться такие меры, как, например, те, что предусмотрены стандартами ИСО 10196 и ИСО 12029.

10.2.3.3 Подготовка документов на микроформах

Перед оцифровкой документы на микроформах должны быть, где это необходимо, очищены от пыли. Оператор должен убедиться в отсутствии каких-либо царапин или дефектов, которые снижали бы читаемость до такой степени, что чтение или обработка оцифрованных документов становятся невозможными.

10.2.3.4 Оцифровка бумажных документов и документов на микроформах

В руководстве пользователя должны быть отражены все детали, относящиеся к сканированию документов, настройке сканера, процессам улучшения изображения и различным элементам процедуры сканирования. Любая технология обработки, используемая для повышения качества получаемой информации, должна быть заранее одобрена инициатором проекта оцифровки и полностью описана в руководстве пользователя системы сканирования.

Руководство пользователя должно охватывать все вопросы, касающиеся авторизованных операций, связанных с модификацией полученных в результате операций оцифровки электронных графических образов.

10.2.3.5 Проверка результатов оцифровки

Руководство пользователя системы оцифровки должно включать процедуру проверки результатов оцифровки.

Проверка результатов оцифровки, как минимум, должна охватывать:

а) качество и аутентичность графических образов в сопоставлении с исходными документами;

б) точность индексирующей информации об оцифрованных документах.

Хотя и допускается осуществление контроля качества непосредственно самими операторами с целью сокращения количества брака, однако настоятельно рекомендуется, чтобы окончательный контроль качества проводился лицами, не являющимися операторами.

Процедуры формирования проверяемой выборки, отражающей отдельные физические элементы, должны соответствовать стандарту ГОСТ Р ИСО 2859.

10.2.4 Контрольная информация о событиях

10.2.4.1 Идентификация документов и партий документов

При оцифровке бумажных документов или документов на микроформах контрольная информация должна включать следующие элементы:

а) уникальный идентификатор документа в информационной системе;

б) количество страниц в документе.

В случае оцифровки партий бумажных документов или документов на микроформах, контрольная информация должна включать в себя следующие элементы:

- идентификатор партии (данный идентификатор должен быть уникальным);
- количество документов, рулонов микроплёнки или микрофиш в данной партии;
- количество оцифрованных страниц или, в случае микроформ, количество оцифрованных кадров.

10.2.4.2 Контрольная информация о процессе захвата документов

В журнале событий, где это уместно, должна быть зафиксирована следующая информация:

- сообщения, полученные от устройства оцифровки (о дате и времени начала оцифровки, о начале обработки партии в случае использования автоматизированной системы, о завершении оцифровки и т.д.);
- объём в байтах оцифрованных документов или партии документов, до и после сжатия изображений (если таковое используется).

10.2.4.3 Состав контрольной информации

Контрольная информация о событиях должна включать, как минимум, перечисленные ниже сведения.

В случае оцифровки бумажных документов:

- а) идентификатор первого документа или первой партии документов, оцифрованных и сохранённых в течение рабочего дня (смены);
- б) идентификатор последнего документа или последней партии документов, оцифрованных и сохранённых в течение рабочего дня (смены);
- с) дата и время прихода и ухода каждого из операторов;
- д) идентификатор первого документа или первой партии документов, оцифрованных и сохранённых каждым из операторов;
- е) идентификатор последнего документа или последней партии документов, оцифрованных и сохранённых каждым из операторов;
- ф) общее количество обработанных страниц;
- г) общее количество необработанных страниц, в том числе тех, что невозможно было оцифровать из-за низкого качества документа (например, низкой контрастности, разрывов и т.п.);
- h) общее количество пустых страниц, если таковые имелись.

В случае оцифровки микроформ:

- идентификатор первой микроформы, оцифрованной и сохранённой в течение рабочего дня (смены);
- идентификатор последней микроформы, оцифрованной и сохранённой в течение рабочего дня (смены);
- дата и время прихода и ухода каждого из операторов;

- идентификатор первой микроформы, оцифрованной и сохраненной каждым из операторов;
- идентификатор последней микроформы, оцифрованной и сохраненной каждым из операторов;
- общее количество обработанных кадров микроформ;
- общее количество необработанных кадров, в том числе тех, что невозможно было оцифровать из-за низкого качества микроформ.

10.3 Аналоговые аудиовизуальные документы на ленточных носителях

10.3.1 Общие положения

Настоящий подраздел относится к информационным системам, которые располагают устройствами для оцифровки оригинальных аналоговых аудио- и видеозаписей.

10.3.2 Подготовка исходных ленточных носителей

Перед оцифровкой магнитных лент их следует проверить с целью оценки состояния носителей и сделанных на них записей.

Такая проверка охватывает:

- физическое состояние лент;
- поведение лент при чтении;
- организацию информации на ленте и качество записей.

10.3.3 Оцифровка аудио- и аудиовизуальных документов

Качество электронных версий документов главным образом определяется параметрами устройств чтения исходных документов и процесса оцифровки (например, свойствами конвертеров и методов дискретизации/кодирования сигнала). В некоторых случаях перед выполнением операций чтения необходимо выполнить процедуры очистки носителей и технического обслуживания оборудования. Должна

быть проведена точная настройка устройств чтения (например, юстировка читающих головок магнитофона, регулирование протяжки видеомэгнитофона).

Используемые для извлечения информации и оцифровки инструменты, а также условия передачи должны быть полностью описаны, включая:

- а) физические характеристики поддерживаемых устройствами оцифровки носителей;
- б) характеристики и настройки устройств чтения (звуковые дорожки, композитный или компонентный аналоговый видеоформат);
- с) спецификации устройств оцифровки.

10.3.4 Обработка аудио- и аудиовизуальной информации

10.3.4.1 Общие положения

В тех случаях, когда необходимо в полной мере сохранить целостность информации, следует исключить или в максимальной возможной степени ограничить применение любых видов обработки, которые способны привести к изменению информации в сравнении с оригиналом.

Когда изменение информации допустимо, например, с целью улучшения качества звука или видеосигнала, то может быть использовано соответствующее программное обеспечение, при условии, что каждая функциональная возможность была протестирована и проверена перед применением. Используемые информационной системой функциональные возможности должны быть полностью отражены в техническом описании.

10.3.4.2 Обработка аудиоматериалов

Для такого рода материалов обычно используются следующие настройки:

- а) настройка скорости протяжки ленты;
- б) регулировка спектрального баланса;
- с) настройка акустического уровня (фиксированное или динамическое сжатие);
- д) удаление нестационарных помех;

- е) широкополосное шумоподавление;
- ф) выбор кодеков для кодирования электронных объектов;
- г) выбор частоты дискретизации.

Любые действия по удалению периодов тишины должны быть тщательно рассмотрены и проверены.

10.3.4.3 Обработка видеоматериалов

Для такого рода материалов обычно используются следующие настройки:

- а) настройка уровня черного;
- б) усиление яркости и цветности;
- с) усиление видеосигнала;
- д) удаление нестационарных помех;
- е) деинтерлейсинг (преобразование чересстрочной развертки в прогрессивную).

Все процессы такого рода должны использоваться с осторожностью, поскольку они влияют на аутентичность оцифрованных аудиовизуальных документов по отношению к оригиналам.

10.3.5 Контрольная информация о событиях

10.3.5.1 Идентификация документов

Для каждого документа должна быть зафиксирована следующая информация:

- а) уникальный идентификатор физического документа в информационной системе;
- б) идентификация записей.

10.3.5.2 Идентификация партий документов

В случае оцифровки партий бумажных документов или документов на микроформах, контрольная информация должны включать следующие сведения:

- а) уникальный идентификатор партии;
- б) количество документов, рулонов или картриджей в каждой партии;
- с) количество оцифрованных лент и записей.

10.3.5.3 Контрольная информация о процедурах захвата и сохранения документов

В случае выполнения подобных процедур, в составе контрольной информации должны быть зафиксированы следующие сведения:

- а) использованные для выполнения операций устройства (система чтения, конвертер и т.д.), выбранные форматы и настройки;
- б) наименования созданных электронных объектов, длительность соответствующих фрагментов записей;
- с) объём в байтах оцифрованных документов или партий документов, до и после сжатия записей (если таковое используется).

10.3.5.4 Контрольная информация об операциях

Журнал аудита операций должен содержать контрольную информацию обо всех операциях, выполняемых в течение каждого дня. Этот журнал должен включать, как минимум, следующие сведения об оцифровке аналоговых аудиовизуальных документов с магнитных лент:

- идентификатор первого документа или первой партии документов, оцифрованных и сохраненных в течение рабочего дня (смены);
- идентификатор последнего документа или последней партии документов, оцифрованных и сохраненных в течение рабочего дня (смены);
- дата и время прихода и ухода каждого из операторов;
- идентификатор первого документа или первой партии документов, оцифрованных и сохраненных каждым из операторов;
- идентификатор последнего документа или последней партии документов, оцифрованных и сохраненных каждым из операторов;
- общее количество обработанных лент или картриджей, а также записей;

- общее количество необработанных лент или фрагментов записей, в том числе тех, что невозможно было оцифровать из-за их низкого качества (например, из-за сдвига дорожек, изломов, растяжений, разрывов, трения и т.п.);
- общее количество пустых лент и длительность пустых фрагментов, если таковые имеются.

10.4 Методы сжатия графических образов, звуковой и аудиовизуальной информации

10.4.1 Виды сжатия

Файлы, содержащие оцифрованные образы исходных аналоговых документов, могут быть сжаты с целью уменьшения объема дискового пространства, необходимого для их хранения.

Существуют два основных метода сжатия: сжатие без потерь (lossless) и сжатие с потерями (lossy).

Сжатие без потерь - это сжатие, выполняемое таким образом, что восстановленный путем распаковки сжатых данных объект побитно идентичен исходному объекту до сжатия.

Сжатие с потерями имеет место, когда восстановленный путем распаковки сжатых данных объект не является идентичным исходному объекту до сжатия. В этом случае часть информации исходного объекта теряется.

10.4.2 Бумажные документы и документы на микроформах

Сжатие с потерями может применяться только для цветных или полутоновых фотографических изображений, если оно не приводит, после цикла сжатие-декомпрессия, к видимым потерям информации.

Сжатие с потерями не должно использоваться для черно-белых документов, часто называемых «офисными», которые в основном содержат тексты и/или векторную (линейную) графику. Для данного типа документов должна

использоваться эталонная тестовая мишень (см. стандарты ИСО 12653-1 и ИСО 12653-2).

Некоторые методы сжатия с потерями позволяют настроить уровень качества. Данный уровень должен быть настроен таким образом, чтобы не было очевидной потери информации в изображении, прошедшем цикл сжатие/хранение/декомпрессия, по сравнению с исходным изображением.

Информационные системы должны предоставлять средства проверки после сжатия файлов, содержащих графические образы.

Вид сжатия и параметры процесса сжатия (если есть) должны сохраняться как неотъемлемая часть файла, содержащего электронный графический образ.

При выборе метода сжатия для решения, предназначенного для хранения документов, следует обратиться к техническому отчету ИСО/ТО 12033 .

Вне зависимости от сделанного выбора, методы сжатия должны быть основаны на стандартах и их спецификации должны быть свободно доступными. В техническом описании должны быть даны ссылки на соответствующие стандарты.

10.4.3 Аудиовизуальные документы

Как правило, аудиодокументы не должны обрабатываться с использованием метода сжатия с потерями.

В случае видеодокументов, учитывая соответствующие объемы хранения и пропускную способность каналов передачи, обычно необходимо применять сжатие с потерями.

Как для аудио-, так и для видеодокументов должны применяться только форматы, стандартизованные Международной организацией по стандартизации (ИСО) в виде серии стандартов MPEG. Выбор для отображения информации конкретных форматов и методов сжатия из числа предлагаемых этими стандартами делается исходя из требований к качеству.

10.5 Преобразование (конверсия) форматов

Должна быть создана таблица, детализирующая исходные форматы, принимаемые системой хранения электронных документов.

Следует выбирать целевые форматы, основанные на общедоступных спецификациях (на стандартах, когда это возможно). Выбор формата, в который преобразуются документы, должен производиться в соответствии с типом электронного документа и теми характеристиками, которые должны быть сохранены или могут не сохраняться после преобразования (конверсии). Важно определить, следует ли сохранять внешний вид (визуальное представление) документов, имеются ли какие-либо ссылки на внешние документы, и должны ли сохраняться математические формулы или внутренние макросы документа.

При выборе нового формата для целей обеспечения долговременной сохранности, а также соответствующих методов конверсии, следует исключить непреднамеренную утрату существенной информации. Параметры конверсии и её выполнение должны контролироваться и протоколироваться в журнале событий, с указанием следующих сведений:

- a) название программы (программ), используемой для конверсии;
- b) название программы (программ), используемых для идентификации и проверки формата по завершении конверсии;
- c) тип события;
- d) дата проведения конверсии;
- e) имя исходного файла;
- f) имя выходного файла;
- g) индикация формата;
- h) результат операции конверсии (т.е. успех или неудача), а при возникновении сбоя – сведения об имевших место аномалиях.

Преобразования формата могут выполняться на различных стадиях процесса хранения: либо при вводе документа в систему хранения электронных документов, либо уже после приема документа на хранение в рамках запланированной конверсии или же в случае, если файловый формат сохраняемого электронного документа устаревает, и из-за этого могут возникнуть проблемы при доступе к нему.

Охват процессов, связанных с форматами хранимых электронных документов, варьируется в зависимости от контрактных соглашений между создателем документального фонда и архивно-документационной службой и от применимой политики хранения:

При вводе документа в информационную систему предпринимаются следующие шаги:

- производятся (либо не производятся) проверки формата при приёме на хранение (на основе таблицы допускаемых системой исходных форматов);
- производится (либо не производится) конверсия формата в момент ввода по результатам проверок либо исходя из контрактных условий, ссылающихся на таблицу целевых форматов, пригодных для длительного хранения.

После ввода в систему хранения электронных документов предпринимаются следующие шаги:

- владелец документов извещается (либо не извещается) в случае устаревания файловых форматов;
- системой хранения электронных документов выполняется (или не выполняется) конверсия в случае устаревания формата.

Проверка формата должна выполняться с помощью инструмента, позволяющего точно идентифицировать, охарактеризовать и проверить формат.

11 Операции с хранимыми документами

11.1 Область применения

Операции с хранимыми документами включают предоставление доступа, реституцию и уничтожение документов.

11.2 Доступ

11.2.1 Общие положения

Базовой операцией доступа является поиск и предоставление соответствующих критериям поиска электронных документов в том формате, в котором они хранятся.

Кроме того, предоставление доступа может включать:

- a) отображение документов на экране;
- b) изготовление копии на бумаге или пленке;
- c) воспроизведение звука в акустических условиях, соответствующих качеству документов;
- d) воспроизведение видеоматериалов в условиях, соответствующих качеству документов.

Методы, используемые для извлечения и отображения документов, должны быть подробно отражены в техническом описании.

При предоставлении доступа не допускается обработка контента документа, за исключением декомпрессии, интерпретации формата и взаимосвязанных технических операций, а также необходимых корректировок физических или программных параметров используемых для доступа устройств.

При необходимости создается свидетельство об аутентичности переданной копии. Такое свидетельство, помимо имени лица, запросившего документы, и имени лица, создавшего свидетельство, включает также метаданные, позволяющие идентифицировать документ и содержащие контрольную информацию о жизненном цикле документа в информационной системе.

11.2.2 Оцифрованные документы

Приложения для ознакомления с документами должны быть независимыми от инструментов, которые использовались для создания сохраняемых документов. Ввиду этого, электронный документ может быть захвачен в программно-аппаратной среде, отличной от среды, используемой для предоставления к нему доступа.

Если в процессе оцифровки бумажных документов или документов на микроформах используется программное обеспечение, которое удаляет формы/фоновое изображение или любые иные фиксированные элементы, принцип аутентичности при предоставлении доступа к документу требует, чтобы восстановленный документ объединял в себе фиксированные и переменные элементы контента. Информационная система должна обеспечить, чтобы использованные при этом версии форм и/или фиксированных элементов были теми же, что были удалены в ходе оцифровки.

11.2.3 Электронные документы, структурированные с помощью языка разметки

Если используются специфические таблицы кодировок, они должны иметься и быть доступными во время предоставления доступа к документу.

Отображение таких документов должно осуществляться путем использования соответствующих инструкций форматирования.

11.2.4 Электронные документы, использующие языки описания внешнего представления

Процессы предоставления доступа должны ограничиваться сборкой различных компонентов документа в соответствии с предписанными правилами отображения и с учетом особенностей целевого устройства отображения, без выполнения каких-либо действий над контентом или какой-либо его обработки.

11.3 Реституция

Реституция документального фонда (полная или частичная) означает возврат принятых на хранение электронных документов их владельцу или надлежащим образом уполномоченной им третьей стороне.

Реституция обязательно должна сопровождаться уничтожением этих документов в системе хранения электронных документов.

Процедура реституции и технические детали передачи документов (формат реституции и выбранные носители информации) должны быть отражены в техническом описании.

11.4 Уничтожение документов

Управление сроками хранения документов осуществляется системой хранения электронных документов либо путем указания срока хранения в метаданных каждого документа, либо путем отсылки к перечню сроков хранения, установленных в зависимости от вида документов. Система должна допускать изменение срока хранения каждого отдельного документа.

По истечении их срока хранения документы должны быть удалены под контролем авторизованного лица и в соответствии с существующими процедурами. Эта операция должна сделать удаленные документы полностью и окончательно недоступными.

Примечание – Дополнительную информацию можно найти в стандартах ГОСТ Р ИСО 15489-1-2019, ГОСТ Р 7.0.101-2018, ГОСТ Р ИСО 30301-2014, ИСО/ТС 19475-3 , а также в спецификациях MoReq2 и MoReq2010.

В случае уничтожения съёмных носителей информации, используемый процесс должен обеспечивать полную недоступность всей записанной на носителе информации.

Всякое сохранение метаданных и контрольной информации, относящихся к уничтоженным документам, должно быть оговорено в договоре или в политике хранения.

12 Аудит системы хранения электронных документов

12.1 Общие положения

12.1.1 Общие положения об аудите

Информационная система и все связанные с ней процедуры должны регулярно проходить аудит, особенно в случае серьёзных изменений в информационной системе. Такой аудит может выполняться как собственным персоналом организации, ответственной за внедрение информационной системы (внутренний аудит), так и/или персоналом, предоставленным третьей стороной (внешний аудит).

Результаты этих аудитов должны сохраняться.

12.1.2 Цели аудита

Аудиты должны подтвердить, что информационная система и процедуры соответствуют положениям настоящего стандарта. Данный контроль соответствия должен охватывать проектирование, внедрение, использование системы и все рабочие процессы.

Кроме того, аудиты должны дать возможность оценить эффективность внедренной информационной системы и ее пригодность для решения задач и исполнения требований в соответствующей сфере деятельности.

Наконец, результаты аудита должны стать той основой, которая, при необходимости, позволит организации повысить уровень соответствия её информационной системы.

12.1.3 Обязанности аудиторов

Аудиторы должны, как минимум:

- а) придерживаться хорошей практики аудита, информировать о настоящих требованиях и разъяснять их;
- б) эффективно выполнять возложенные на них задачи;

- с) документировать результаты;
- д) докладывать о выводах, сделанных по итогам аудита.

Аудиторы должны быть беспристрастными и неподверженными какому-либо влиянию, способному сказаться на их объективности.

12.1.4 Персонал, ответственный за проведение аудита

Сведения о квалификации, обучении и опыте каждого лица, выполняющего или помогающего в выполнении операций аудита, должны собираться и поддерживаться ответственной за аудиторов организацией.

В частности, аудиторы должны иметь многолетний профессиональный опыт в области управления электронными документами и информацией, а также организации их хранения, значительная часть которого должна быть связана с проектной или консультационной деятельностью в сфере электронных систем управления документами.

Как внутренние, так и внешние аудиторы должны обладать следующими знаниями и навыками, необходимыми для проведения процесса аудита:

- владение методами сбора информации, проведения опросов и собеседований, анализа материалов и подготовки отчетов;
- владение различными методами управления процессом аудита, охватывающими такие аспекты, как планирование, выбор методологии, организация работ, информирование, взаимодействие с персоналом.

Знания и навыки аудиторов в совокупности должны быть достаточными для того, чтобы охватывать все типы содержащихся в информационной системе документов. В тех случаях, когда для аудита хранения отдельных типов документов требуются специальные технические знания (звуковые и аудиовизуальные документы и т.д.), имеющие соответствующие компетенции специалисты привлекаются по мере необходимости.

12.1.5 Управление документацией

Организация должна поддерживать информационную систему, позволяющую управлять всей охватываемой подобным аудитом документацией, и обеспечивающую, что:

- а) актуальные версии необходимой документации доступны в соответствующих количествах во всех точках, где проводятся операции с информационной системой;
- б) все изменения или дополнения в документации должны быть надлежащим образом авторизованы и должны обрабатываться таким образом, чтобы обеспечить быстрые и непосредственные действия персонала;
- с) устаревшая документация незамедлительно изымается со всех точек распространения и использования в организации и уничтожается (в исключительных случаях устаревшая документация, которую необходимо сохранить для юридических или исторических целей, должна быть надлежащим образом идентифицирована и сохранена).

12.1.6 Документирование операций аудита

Организация должна задокументировать всю совокупность результатов операций аудита. Документы должны описывать способы проведения каждой операции аудита.

Все документы должны надежно сохраняться в течение соответствующего периода времени.

12.2 Внутренний аудит

Когда аудит проводится подчиненным организации персоналом, организация должна создать и быть в состоянии представить своё описание, четко показывающее распределение обязанностей и иерархическую структуру организации, и демонстрирующее, в том числе, независимость исполнителей ролей аудиторов от исполнителей ролей в оперативной деятельности.

12.3 Внешний аудит

Сторонние организации, проводящие аудиты информационных систем, должны иметь достаточный и адекватный опыт и знания в области проектирования и внедрении информационных систем, предназначенных для обеспечения сохранности электронных документов.

Выполняющий операции аудита персонал должен иметь соответствующую квалификацию, подготовку и опыт для надлежащего проведения аудита систем хранения электронных документов.

Сторонние организации должны принять все необходимые меры на всех уровнях своей организационной структуры для обеспечения конфиденциальности собранной в ходе аудита информации.

13 Хранение документов доверенной третьей стороной

13.1 Деятельность доверенной третьей стороны – поставщика услуг хранения

Правила, применяемые к внутренним решениям, в равной степени применимы в отношении доверенных третьих сторон – поставщиков услуг хранения электронных документов. При передаче документов на ответственное хранение доверенной третьей стороне, организация должна убедиться, что используемые той методы и процедуры обеспечивают безопасность, целостность и долговременную сохранность электронных документов, и что исполнение всех распоряжений сопровождается созданием соответствующих свидетельств. В Приложении С приведены принципы, касающиеся предлагаемых общих условий обслуживания.

Прежде, чем передать какие-либо документы на хранение доверенной третьей стороне, следует удостовериться в том, что:

- a) доверенная третья сторона способна обеспечить соответствие требованиям настоящего стандарта;
- b) используемая третьей стороной политика хранения соответствует политике хранения организации;

с) процедуры безопасности третьей стороны соответствуют процедурам безопасности организации.

Доверенная третья сторона может:

- либо обеспечить прием на хранение самих электронных документов (включая получение и регистрацию всех электронных документов, документирование операций, хранение электронных документов и их метаданных), взять на себя ответственность за операции конверсии, реализовать процедуры репликации, обеспечить предоставление доступа к документам и их возврат (реституцию);

- либо обеспечить хранение только хешей (дайджестов) документов (включая получение, проверку и регистрацию хешей электронных документов, документирование операций), - при этом ответственность за хранение и обеспечение сохранности соответствующих этим хешам электронных документов продолжает нести организация – клиент доверенной третьей стороны.

В обоих случаях доверенная третья сторона создает свидетельства своей деятельности. Тип и частота предоставления доверенной третьей стороной этих свидетельств клиенту должны быть указаны в каждом договоре с третьей стороной.

Доверенная третья сторона должна хранить вторые экземпляры этих свидетельств в соответствии с требованиями настоящего стандарта.

Доверенная третья сторона – поставщик услуг хранения должна внедрить систему, которая, помимо соответствия требованиям настоящего стандарта, также должна:

- обеспечить уникальную и надежную идентификацию каждого из своих клиентов;

- обеспечить конфиденциальность принятых на ответственное хранение документов и метаданных, в частности, путем использования информационной системы, реализованной таким образом, что клиент третьей стороны не имеет возможности читать, писать, изменять или удалять какие-либо документы другого клиента этой третьей стороны;

- выдавать свидетельства для каждой операции приема на хранение;

- выполнять операции уничтожения документов только после предварительного уведомления клиента и, по их завершении, выдавать соответствующие свидетельства;

- вести для каждого клиента журнал аудита жизненного цикла документального фонда, который может быть представлен в качестве доказательства в случае спора;

Обмен данными между организацией и третьей стороной должен быть защищен посредством применения надлежащих мер и средств, т.е. путем использования строгой аутентификации (strong authentication), шифрования и контроля целостности.

Третья сторона должна поручиться, что она не будет анализировать или обрабатывать электронные документы, переданные ей на ответственное хранение (например, проводить конверсию формата), если только этого явно не потребует клиент.

По соображениям конфиденциальности, организация может счесть необходимым предварительное шифрование документов и, где это уместно, метаданных. В таком случае возможности использования поисковых запросов для доступа к документам могут быть ограничены.

13.2 Типовой договор об оказании услуг

13.2.1 Содержание договора об оказании услуг

В договоре об оказании услуг, заключенном с доверенной третьей стороной - поставщиком услуг хранения, должны быть отражены следующие вопросы:

- a) ссылка на данный стандарт с указанием исполненных требований;
- b) ссылка на политику хранения;
- c) описание процедур хранения;
- d) описание инфраструктуры информационной системы;
- e) процедуры доступа к контрольной информации о функционировании информационной системы;
- f) методы, используемые третьей стороной для обеспечения конфиденциальности данных организации;

g) методы и носители информации, используемые для передачи клиентом на хранение электронных документов и их метаданных;

h) методы и средства, используемые для проведения, где это уместно, конверсии форматов;

i) процедуры транспортировки содержащих документы носителей информации, где это уместно;

j) договоры страхования, заключенные третьей стороной для покрытия возможного ущерба, связанного с её деятельностью.

Хотя содержание договора об оказании услуг свободно определяется сторонами, тем не менее, в него должно быть включено содержание подразделов с 13.2.2 по 13.2.13.

13.2.2 Продолжительность оказания услуг

Должен быть указан срок, на который заключен договор об оказании услуг между доверенной третьей стороной – поставщиком услуг хранения и клиентом, а также условия продления и расторжения договора.

13.2.3 Сроки хранения документов

Доверенная третья сторона должна взять на себя обязательство соблюдать установленные сроки хранения, пока это позволяют действующие договорные взаимоотношения. Третья сторона должна быть в состоянии продемонстрировать договорную и техническую возможность реституции документов либо их передачи другому поставщику услуг, а также интероперабельность своего решения в целях обеспечения сохранности документов в течение согласованных сроков.

13.2.4 Качество оказания услуг

Доверенная третья сторона должна взять на себя обязательство обеспечить определенный уровень качества оказания услуг и поддержки клиента. Данное обязательство касается уровня доступности/готовности принимать документы

на хранение и предоставлять к ним доступ, и может предусматривать штрафные санкции за неисполнение условий договора.

13.2.5 Обеспечение безопасности и защита данных

Доверенная третья сторона должна:

- а) сохранять в течение предусмотренного договором срока все переданные клиентом на ответственное хранение электронные документы в согласованной форме и форматах;
- б) обеспечить безопасность и целостность электронных документов;
- с) взять на себя обязательство выполнять процессы миграции носителей информации, которые могут потребоваться для обеспечения читаемости электронных документов;
- д) предоставить сервис защищённого доступа ко всем находящимся на ответственном хранении объектам;
- е) сохранять контрольную информацию обо всех операциях, связанных с оказанием предусмотренных договором услуг;
- ф) обеспечить безопасность и целостность журнала аудита жизненного цикла документального фонда и журнала событий.

13.2.6 Информирование и консультирование

Третья сторона должна информировать своего клиента о необходимости поддерживать совместимость между собственными информационными системами клиента и теми объектами, которые находятся на ответственном хранении по поручению клиента. Доверенная третья стороне может предложить дополнительные услуги для решения этой задачи.

Третья сторона должна информировать клиента о любых операциях конверсии и о технических изменениях в используемых информационных системах; а также о любом воздействии, которое те могут оказать на доступность или совместимость с оборудованием клиента, или же на обмен данными и на обеспечение сохранности переданных третьей стороне данных.

13.2.7 Переход к другому поставщику и непрерывность ответственного хранения

Если находящиеся на ответственном хранении электронные документы клиента передаются по его распоряжению другой третьей стороне – поставщику услуг хранения, то эта другая третья сторона должна быть способна обеспечить, как во время, так и после операции передачи, сохранение документами их ключевых свойств. С этой целью:

- первоначальный поставщик услуг хранения должен обеспечить передачу всей совокупности находившихся на его ответственном хранении документов и взаимосвязанных с ними данных, гарантируя их целостность;

- в любом случае первоначальный поставщик услуг хранения должен разместить в месте или с помощью средств, доступных для его клиента или любой уполномоченной клиентом стороны, информацию и технические данные, позволяющие осуществить восстановление данных, а также принять все необходимые меры для того, чтобы его клиент в течение разумного периода времени имел возможность получить назад переданные на хранение документы (осуществить реституцию).

13.2.8 Переносимость

По окончании действия договора или в случае прекращения деятельности доверенной третьей стороны – поставщика услуг хранения, третья сторона должна быть способна провести реституцию (возврат) клиенту всей совокупности электронных документов и связанных с ними данных, полностью и в том же техническом состоянии, в котором они были на момент приема на хранение в систему хранения электронных документов. Доверенной третьей стороне запрещается сохранять у себя копии возвращенных документов.

Должен быть предусмотрен возврат журналов аудита/контрольной информации.

Положение о переносимости позволяет избежать зависимости клиента от доверенной третьей стороны – поставщика услуг хранения, предусматривая

в договоре либо переход исполнения переданной внешнему поставщику функции хранения к другому поставщику услуг, либо возобновление выполнения данной функции собственными силами клиента.

Данное положение должно включать, как минимум:

- а) использование третьей стороной современных стандартных и имеющихся на рынке технических средств (таких, как архитектура, аппаратное и программное обеспечение, протоколы и т.д.);
- б) организация третьей стороной передачи исполнения функции хранения самому клиенту либо другой доверенной третьей стороне – поставщику услуг хранения;
- в) размещение третьей стороной в месте или с помощью средств, доступных для его клиента или любой уполномоченной клиентом стороны, информации и технических данных, позволяющих осуществить восстановление данных;
- г) стоимость переносимости;
- д) время, необходимое для выполнения всех операций переносимости, начиная от момента подачи запроса;
- е) регулярная актуализация всех элементов, связанных с переносимостью.

13.2.9 Реституция

По прекращении договорных обязательств о хранении документов, третья сторона обязуется вернуть клиенту все хранимые документы, не оставляя себе их копий. Тем не менее, по специальной просьбе клиента его документы могут продолжать храниться третьей стороной в течение дополнительного периода времени.

13.2.10 Конфиденциальность и защита персональных данных

Третья сторона должна обеспечить конфиденциальность информации, хранение которой ей было доверено, а также любой иной информации, которая могла стать ей известной в течение договорных отношений с клиентом.

Эта информация может быть получена третьей стороной в результате доступа или в ходе операций с переданными ей на ответственное хранение документами, или же вытекать из знаний об информационных системах организации-клиента - как полученных на основе собственных наблюдений, так и предоставленных её клиентом.

Третья сторона должна принять все необходимые меры для обеспечения конфиденциальности информации, которая может стать ей известна в ходе проведения работ по техническому обслуживанию.

Такая информация должна раскрываться только указанным клиентом лицам, за исключением ситуаций, когда законодательство обязывает поставщика услуг хранения передавать эту информацию иной стороне.

13.2.11 Страхование профессиональной ответственности

Третья сторона должна заключить договор страхования для покрытия всех рисков, связанных с её гражданской ответственностью. Эта страховка должна обеспечить финансовую защиту деятельности третьей стороны в случае, если будет поставлено под сомнение выполнение ею своих обязательств.

Третья сторона должна поддерживать такое страхование до тех пор, пока действует договор об оказании услуг.

Третья сторона может приобрести дополнительную страховую защиту на случай сбоя информационной системы.

13.2.12 Субподряд

В случае передачи на субподряд всей или части услуги, являющейся предметом договора, доверенная третья сторона – поставщик услуг хранения должна проинформировать своего клиента и несёт ответственность за услуги, оказываемые субподрядчиками.

13.2.13 Аудит

Положение, касающееся проведения аудита, должно соответствовать требованиям настоящего стандарта (см. раздел 12).

14 Поставщики услуг

14.1 Общие положения

В данном разделе рассматриваются решения для хранения документов, для которых некоторые услуги предоставляются субподрядчиками, не являющимися доверенными третьими сторонами – поставщиками услуг хранения. В Приложении С приведены принципы, касающиеся предлагаемых общих условий обслуживания.

Организация, внедрившая информационную систему, продолжает нести ответственность за всю систему в целом и должна обеспечить, чтобы все предоставляемые субподрядчиками услуги соответствовали требованиям настоящего стандарта в отношении порученных им обязанностей.

Авторизованное лицо, ответственное за выбор поставщика услуг, должно предоставить выбранному субподрядчику устанавливающий требования документ, а субподрядчик должен принять на себя обязательство соблюдать эти требования.

Процедуры поставщика услуг должны быть систематически проанализированы, а его операции должны регулярно инспектироваться.

14.2 Требования к субподрядчику

Прежде чем воспользоваться услугами субподрядчика, следует убедиться в том, что:

- субподрядчик способен выполнить требования настоящего стандарта в отношении оказываемых им услуг;
- процедуры субподрядчика соответствуют политике хранения организации;
- создаваемая субподрядчиком контрольная информация может использоваться в информационной системе организации;

– политики безопасности субподрядчика согласуются с соответствующими политиками организации.

14.3 Договор с субподрядчиком

Договор должен содержать, как минимум, следующую информацию:

- а) ссылку на настоящий стандарт, т.е. «ИСО 14641»;
- б) описание используемых процедур;
- с) описание инфраструктуры, используемой в связи с предоставленной услугой;
- д) критерии, используемые для контроля качества;
- е) доступ к журналам событий в информационной системе субподрядчика;
- ф) меры, принятые поставщиком услуг для обеспечения конфиденциальности и безопасности хранимых им данных организации;
- г) методы и носители информации, используемые для передачи электронных документов и соответствующих метаданных между организацией и субподрядчиком;
- h) методы и средства, используемые для конверсии формата, где это уместно;
- і) процедуры транспортировки содержащих документы носителей информации, где это уместно;
- ј) страховые полисы, приобретенные субподрядчиком для покрытия возможного ущерба, связанного с его деятельностью.

14.4 Передача данных по телекоммуникационным сетям

Если для передачи документов между владельцем и субподрядчиком используются открытые сети, то необходимо использовать надлежащие методы аутентификации, обеспечения целостности данных и конфиденциальности.

Приложение А

(справочное)

Политика хранения

Политика хранения описывает юридические, функциональные, эксплуатационные, технические требования и требования по безопасности к внутренней или внешней системе хранения, в том числе цели, задачи и обязательства этой системы.

Политика хранения формализует цели, которые должны быть достигнуты внутренней или внешней архивно-документационной службой, и обязательства, которые она должна выполнять. Политика хранения должна определять:

а) услуги, предоставляемые владельцам и пользователям документов по приему-передаче и реституции документов, включая виды услуг, уровни обслуживания, тип хранения (оперативное/промежуточное/архивное), форматы электронных документов, условия, объемы и периодичность передачи партий документов и т.д.;

б) обязательства, возложенные на все вовлечённые стороны, в первую очередь на саму архивно-документационную службу. Обязательства других сторон являются теми минимальными требованиями, которые те должны соблюдать с тем, чтобы архивно-документационная служба могла оказывать услуги хранения в соответствии с политикой хранения;

с) функциональные возможности, реализуемые архивно-документационной службой с целью предоставления данных услуг (функция приема-передачи на хранение, функция хранения и т.д.) и соответствующая функциональная структура (связи между функциями, потоки информации и т.д.);

д) применимые правила безопасности, соответствующие каждому уровню обслуживания и каждой функции, основанные на организационных, практических и технических соображениях.

Политика хранения – это, прежде всего, общая функциональная концепция и, как таковая, она не должна зависеть от конкретных методов, используемых для реализации определенных операций.

Политика хранения представляет собой документ, который даёт всем вовлечённым сторонам (внутренним или внешним по отношению к архивно-документационной службе) четкое представление об обязательствах архивно-документационной службы. Из него

вытекают практические соображения, связанные с оказанием услуги хранения, в том числе касающиеся таких вопросов, как:

- передача документов на хранение;
- идентификация и аутентификация источника документов;
- доступ к документам;
- поиск и отображение документов;
- реституция документов;
- целостность документов;
- читаемость документов;
- обеспечение долговременной сохранности документов;
- прослеживаемость операций приёма на хранение, реституции и уничтожения;
- формирование свидетельств;
- обеспечение непрерывности деловой деятельности и/или её восстановление после чрезвычайных ситуаций, вызванных как случайными обстоятельствами, так и злонамеренными действиями;
- преднамеренное уничтожение документов.

Приложение В

(справочное)

Декларация практики хранения документов

В декларации практики хранения объясняются методы и процессы, реализованные для достижения целей безопасности политики хранения.

В декларации практики хранения следует описать, каким образом архивно-документационная служба организации и/или доверенной третьей стороны – поставщика услуг хранения обеспечивает соответствие требованиям политики хранения в отношении аспектов условий хранения, материалов, процессов, операций и методов.

Декларация практики хранения должна содержать подробное описание практики оперативной работы архивно-документационной службы организации либо доверенной третьей стороны – поставщика услуг хранения при управлении процессами хранения.

В декларации практики хранения установленные в политике хранения принципы безопасности должны получить своё отражение:

- в принципах безопасности оперативной деятельности на уровне различных подразделений архивно-документационной службы, а также
- в правилах безопасности, которые должны быть реализованы с целью соблюдения этих принципов.

Эти принципы и правила могут либо быть описаны непосредственно в декларации практики хранения, особенно если они касаются деятельности архивно-документационной службы; либо в декларации практики хранения может даваться ссылка на более общую политику обеспечения безопасности информационных систем.

Декларация практики хранения должна, как минимум, установить взаимосвязь между сформулированными в соответствующей политике хранения принципами - и принципами и правилами оперативной работы, демонстрируя всесторонний охват вопроса.

Если политика хранения формулируется независимо от специфических особенностей конкретной среды использования системы хранения электронных документов, то декларация практики хранения пишется с учетом организационной структуры, рабочих процессов и материально-технической оснащенности архивно-документационной службы организации или доверенной третьей стороны - поставщика услуг хранения.

Декларация практики хранения всегда предоставляется поставщиком услуги, то есть архивно-документационной службой организации или доверенной третьей стороны - поставщика услуг хранения.

Декларация практики хранения в принципе является конфиденциальным внутренним документом, касающимся только архивно-документационной службы. Однако, в качестве дополнения к политике хранения, архивно-документационная служба может предоставить выдержки из своей декларации практики хранения.

В декларации практики хранения описывается, каким образом архивно-документационная служба организации или доверенной третьей стороны - поставщика услуг хранения намерена надлежащим образом выполнить свои обязанности. Это делает декларацию особенно полезной при проведении аудита, поскольку она облегчает работу аудитора и позволяет сократить длительность аудита.

Приложение С

(справочное)

Общие условия обслуживания

Пользователи услуг хранения в каких-то случаях могут иметь доступ только к политике хранения организации или доверенной третьей стороны – поставщика услуг хранения, и для них этот документ может оказаться трудным для понимания.

Ввиду этого было бы полезно предоставить пользователям дополнительный упрощенный документ, разъясняющий и помогающий понять ключевую информацию, которая им необходима для принятия обоснованных решений.

Общие условия обслуживания должны ссылаться на имеющиеся руководства пользователя. Чтобы оставаться ясными и понятными, такие руководства должны описывать только те функциональные возможности, которые необходимы для поддерживаемых операций, - хотя они могут ссылаться на более общие руководства, если это будет сочтено полезным.

Архивно-документационная служба организации или доверенной третьей стороны – поставщика услуг хранения должна предоставлять пользователям свои общие условия обслуживания.

Приложение ДА
(справочное)

**Сведения о соответствии ссылочных международных стандартов
национальным стандартам Российской Федерации**

Таблица ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 2859	IDT	ГОСТ Р ИСО 2859 (все части) «Статистические методы. Процедуры выборочного контроля по альтернативному признаку» и ГОСТ Р 50779.70–2018 «Статистические методы. Процедуры выборочного контроля по альтернативному признаку. Введение в стандарты серии ГОСТ Р ИСО 2859»
ISO 8601	MOD	ГОСТ Р 7.0.64-2018 «Система стандартов по информации, библиотечному и издательскому делу. Представление дат и времени. Общие требования»
ISO/TR 12033	—	*
ISO 12653-1	—	*

Окончание таблицы ДА.1

Обозначение ссылочного международного стандарта, документа	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO 12653-2	—	*
* Соответствующий национальный стандарт отсутствует. Примечание – В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: – IDT – идентичные стандарты. – MOD – модифицированные стандарты.		

Библиография

- [1] ISO 6196-8, Micrographics — Vocabulary — Part 8: Use
- [2] ISO 10196, Document imaging applications — Recommendations for the creation of original documents
- [3] ISO 12029, Document management — Machine-readable paper forms — Optimal design for user friendliness and electronic document management systems (EDMS)
- [4] ISO 14721, Space data and information transfer systems — Open archival information system (OAIS) — Reference model
- [5] ISO 15489-1, Information and documentation — Records management — Part 1: Concepts and principles
- [6] ISO/TR 15801, Document management — Electronically stored information — Recommendations for trustworthiness and reliability
- [7] ISO 19005 (all parts), Document management — Electronic document file format for long-term preservation
- [8] ISO/TR 22957, Document management — Analysis, selection and implementation of electronic document management systems (EDMS)
- [9] ISO/IEC 13346 (all parts), Information technology — Volume and file structure of write-once and rewritable media using non-sequential recording for information interchange
- [10] ISO/IEC 13490 (all parts), Information technology — Volume and file structure of read-only and write-once compact disk media for information interchange
- [11] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements
- [12] IEC 61000-4, Electromagnetic compatibility (EMC) — Part 4: Testing and measurement techniques
- [13] ETSI TS 101 733, Electronic Signatures and Infrastructures (ESI) Electronic Signature Formats, European Telecommunications Standardization Institute
- [14] ETSI TS 101 903, Electronic Signatures and Infrastructures (ESI) XML Advanced Electronic Signatures (XAdES), European Telecommunications Standardization Institute

- [15] MoReq2, Model Requirements for the Management of Electronic Records.
Available at: www.moreq2.eu

УДК 004.912:004.932:006.354

ОКС 37.080

Ключевые слова: архивное дело, доверенная третья сторона, документные процессы, документные системы, долговременная сохранность, информационная безопасность, системы хранения электронных документов, СХЭД, СЭД, электронная архивация, электронные архивы, управление документами, ECM

Руководитель организации-разработчика

Общество с ограниченной ответственностью «ЭОС Тех»

Генеральный директор

_____ Е.П. Пушкарёв

Руководитель разработки

к.и.н., Председатель Совета директоров,

Председатель ПК 6 «Жизненный цикл

электронного документооборота» ТК 459 _____ В.Э. Баласанян

Исполнитель

к.и.н., ведущий эксперт по управлению документацией

Общества с ограниченной ответственностью «ЭОС Тех»,

эксперт ИСО, член Международного Совета Архивов,

член Гильдии управляющих документацией

и ARMA International

_____ Н.А. Храмцовская