Федеральное архивное агентство
(Росархив)

Государственное учреждение
Всероссийский научно-исследовательский институт
документоведения и архивного дела
(ВНИИДАД)

Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов

Москва 2012

Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов/ руководитель темы Г.З. Залаев, ответственный исполнитель темы Н.В. Глищинская, исполнитель С.Л. Новиков.

Методические рекомендации по организации работы и технологическому оснащению хранилищ электронных документов, разработаны по государственному контракту с Федеральным архивным агентством № 55 от 22.05.2012 г. ФЦП «Культура России» (2012–2018 гг.) Проведение научно-исследовательской работы (НИР) на тему «Разработка методических рекомендаций по организации работы и технологическому оснащению хранилищ электронных документов».

СОДЕРЖАНИЕ

Введение

Развитие информационных технологий привело к возникновению и стремительному росту электронных документов. Электронные документы появляются как цифровые копии традиционных архивных документов в результате технологии оцифровки, а также возникают и проходят жизненный путь в системах электронного документооборота. Федеральное архивное агентство в рамках программы информатизации архивной отрасли на 2011-2020 гг. запланировало проведение целого ряда мероприятий и научно-исследовательских работ, целью которых должно стать формирование комплекса нормативно-методических материалов (Инструкций, Методических рекомендаций, Правил и т.п.), направленных на унификацию и регламентирование процессов перевода архивных документов в цифровой формат (создание электронных копий архивных документов), а также обеспечению взаимодействия с системами электронного документооборота ФОИВ.

Методические рекомендации посвящены основным вопросам хранения электронных документов в Центре хранения электронных документов (ЦХЭД) и определяют технические требования к системе хранения электронных документов, компьютерной технике и программному обеспечению для единой системы хранения электронных документов архивной отрасли, а также функциональные и технические требования к ней (далее – Рекомендации).

Рекомендации основаны на анализе методологии построения систем обработки и хранения электронной информации различного применения, практическом опыте и материалах, представленных в литературе.

Рекомендации предназначены для использования при проектировании хранилища данных (электронных документов) центра хранения электронных документов, а также при проектировании хранилища цифровых копий

документов федеральных архивов при централизованном их хранении в ЦХЭД.

Рекомендации предполагают обеспечение сопряжения разрабатываемого комплекса компьютерного оборудования и программного обеспечения с инфраструктурой системы электронного документооборота федеральных органов исполнительной власти (СЭД ФОИВ) в целях приема на государственное хранение электронных документов из СЭД ФОИВ, а также оказания государственных услуг в сфере обеспечения архивной информацией органы исполнительной власти, организаций и граждан в соответствии с Государственной программой «Информационное общество (2011-2020 годы)», утвержденной Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р.

В Рекомендациях рассматриваются следующие вопросы:

- Требования к системам электронного документооборота ФОИВ с целью организации его взаимодействия с системой архивного хранения электронных документов по передаче и приему электронных документов из СЭД ФОИВ.
- Хранение и использование электронных документов в федеральных архивах (на примере РГАНТД).
- Применимость «облачных» технологий и систем управления цифровым контентом при организации хранения и использования электронных документов, а также анализ требований к аппаратным и программным платформам для хранения больших массивов электронных документов.
- Технические и технологические требования по передачи электронных документов в хранилище данных центра хранения электронных документов.

- Передача электронных документов в центр хранения электронных документов от СЭД ФОИВ и федеральных архивов.
- Рекомендации по созданию централизованного хранилища электронных документов и по организации их использования.

Настоящие Методические рекомендации разработаны в соответствии со следующими документами:

Правила организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных и муниципальных архивах, музеях и библиотеках, организациях Российской академии наук (утв. 18.01.2007).

Государственные стандарты (ГОСТ) Российской Федерации.

1. Взаимодействие СЭД ФОИВ и ЦХЭД

Характеристики системы хранения данных в ЦХЭД в значительной мере определяются характеристиками систем электронного документооборота федеральных органов исполнительной власти (СЭД ФОИВ). Приказом Министерства связи и массовых коммуникаций (Минкомсвязь) РФ № 221 от 02.09.2011 утверждены “Требования к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающие, в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения” (далее – Требования). (Приложение 1).

Требования, утвержденные приказом Минкомсвязи, распространяются на внедряемые СЭД и на внедренные уже системы при их оценке (пункт 2 Требований).

Пункт 3 Требований определяет требования масштабируемости и производительности СЭД. Доступ к СЭД ФОИВ должен осуществляться в течение не более 3 секунд, доступ к карточке документа (описания документа) — в течение не более 5 секунд. Данное положение предъявляет высокие требования к аппаратной и программной платформам системы, а также к архитектуре системы и к системам, которые взаимодействуют с СЭД ФОИВ.

Требование к простою при сбоях и перезагрузке системы составляет 30 мин. Данное требование определяет качество системы хранения данных (надежность и отклик, систему резервирования и т.д.), а также требование к организации работ по обслуживанию системы и подготовку обслуживающего систему технического персонала. При этом производится автоматическое уведомление должностного лица ФОИВ, использующего СЭД ФОИВ (пользователь СЭД ФОИВ), о сбое в СЭД ФОИВ. Коэффициент надежности СЭД ФОИВ определяется как не менее 0,98.

Таким образом, особое внимание в этом контексте к созданию системы приема электронных документов на государственное хранение (интерфейса между СЭД ФОИВ и системой государственного хранения электронных документов – центром хранения электронных документов (ЦХЭД)), параметры функционирования которой не приводили бы к ухудшению данных требований.

Пункт 3 Требований определяет срок хранения документов в базе данных СЭД. Объем базы данных для хранения электронных документов должен обеспечивать хранение всех электронных документов, обрабатываемых в ФОИВ за период не менее 5 лет.

Данное требование определяет возможные объемы и структуру системы хранения данных ЦХЭД, ее отказоустойчивость, резервирование и безопасность, а также масштабируемость. При этом СЭД ФОИВ управляет всеми документами федерального органа исполнительной власти, включая проекты документов, кроме документов, содержащих сведения, составляющие государственную тайну (пункт 4 Требований).

Сроки хранения документов, включенных в соответствующие разделы (подразделы) СЭД ФОИВ устанавливаются в соответствии с Перечнем типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения, утвержденным приказом Министерства культуры Российской Федерации от 25.08.2010 № 558 (зарегистрирован в Министерстве юстиции Российской Федерации 8 сентября 2010 г., регистрационный № 18380) (пункт 19 Требований).

Важным для организации взаимодействия СЭД ФОИВ с ЦХЭД является положение Требований сформулированных в пункте 5 о взаимодействии СЭД ФОИВ и системами межведомственного электронного документооборота (МЭДО) и межведомственного электронного взаимодействия (СМЭВ):

Взаимодействие СЭД ФОИВ с системой МЭДО регламентируется техническими требованиями к организации взаимодействия системы межведомственного электронного документооборота с системами электронного документооборота федеральных органов исполнительной власти, утвержденными распоряжением Правительства Российской Федерации от 2 октября 2009 г. № 1403-р (Собрание законодательства Российской Федерации, 2009, № 41, ст. 4818).

Пункт 12 Требований определяет форматы электронных документов СЭД ФОИВ: СЭД ФОИВ должна обеспечивать работу с электронными документами следующих форматов файлов:

- pdf,
- rtf,
- doc,
- tiff.

Также в СЭД ФОИВ допускается применение и других форматов файлов.

Таким образом, хранилище электронных документов ЦХЭД должно обеспечивать поддержку выше обозначенных форматов pdf, rtf, doc, tiff, а также предусматривать возможность работы с электронными документами других форматов.

Важным для организации использования электронных документов в центре хранения электронных документов при их использовании является (пункт 14 Требований) наличие интерфейса, позволяющего подключать средства электронных подписей, получившие подтверждение соответствия требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880).

СЭД ФОИВ поддерживает передачу электронных документов «на хранение в иное хранилище» (пункт 20г. Требований).

Из этого положения следует возможность взаимодействия между СЭД ФОИВ и хранилищем электронных документов ЦХЭД.

Требования к информационной безопасности СЭД ФОИВ, в том числе при обработке служебной информации ограниченного распространения определяется разделом 3 Требований.

Для защиты служебной информации ограниченного распространения должны использоваться сертифицированные в соответствии с требованиями безопасности информации технические и (или) программные средства защиты информации.

СЭД ФОИВ должна соответствовать требованиям национального стандарта Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» и требованиям по технической защите конфиденциальной информации.

СЭД ФОИВ должна обеспечивать контроль доступа к документам, что требует необходимость протоколирования и сохранения контрольной информации о предоставлении доступа и о других операциях с документами и метаданными в СЭД ФОИВ.

СЭД ФОИВ не должна иметь незащищенного подключения к информационно-телекоммуникационной сети Интернет в соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110; 2008, № 43, ст. 4919; 2011, № 4, ст. 572).

Анализ требований к системам ЭДО ФОИВ “Требования к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающие, в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения” позволил определить требования к хранилищу электронных документов ЦХЭД. Основными, из которых являются использование сертифицированных в соответствии с требованиями безопасности информации технических и программных средств защиты информации, обеспечение управления документами, имеющих электронные цифровые подписи и соответствие требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [1], а также использование защищенного канала подключения к сети Интернет.[2]

Для уточнения характеристик хранилища электронных документов ориентированного на конкретную систему ЭДО ФОИВ рекомендуется провести анкетирование федерального органа исполнительной власти. (Приложение 2).

[1] ФЗ от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». (Собрание законодательства Российской Федерации, 2011, № 15, ст. 2036; № 27, ст. 3880).

[2] Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110; 2008, № 43, ст. 4919; 2011, № 4, ст. 572).

2. Хранение и использование электронных документов в федеральных архивах (на примере РГАНТД)

В Российском государственном архиве научно-технической документации накоплен многолетний опыт по хранению и управлению цифровым контентом.

Работы ведутся в нескольких направлениях.

С 1999 г. в архиве с целью создания электронного фонда пользования (ЭФП) ведутся работы по оцифровке архивных документов (видео-, фоно-, фотодокументов, документов на бумажной основе). Учет и хранение ЭФП производится на внешних носителях информации (специализированные CD и DVD диски для архивного хранения). В архиве разработаны временные правила по приему, учету, хранению и использованию внешних носителей информации с ЭФП. Оперативное хранение оцифрованных, но не переданных на хранение архивных документов (мастер-копий) ведется в сетевой системе хранения данных NAS (Network Attached Storage). Также в системе хранения данных с соблюдением принципа иерархического учета и описания архивных документов хранятся рабочие копии оцифрованных архивных документов, а также массив производных электронных копий архивных документов для включения в базу данных РГАНТД – Автоматизированную информационно-поисковую систему с цифровыми копиями архивных документов (АИПС ЦКД).

В РГАНТД ведутся плановые работы по сохранности информации, введенной во все базы данных архива. С целью оперативного использования сохранность информации производится на сервера РГАНТД.

С 2001 г. на серверах web-узла РГАНТД располагается отраслевой портал «Архивы России», а с 2009 г. официальный сайт Росархива, который является официальным сайтом ФОИВ и к нему соответственно применяются

Требования к технологическим, программным и лингвистическим средствам обеспечения пользования официальными сайтами федеральных органов исполнительной власти, утвержденные приказом Министерства экономического развития Российской Федерации (Минэкономразвития России) от 16 ноября 2009 г. № 470, в т.ч. и к резервному копированию всей размещенной на официальном сайте информации и электронных журналов учета операций.

В РГАНТД используется полное резервное копирование (Full backup) с цепочкой версий – ежедневное, еженедельное и ежемесячное. Копии хранятся на магнитной ленте и на дисках сервера.

Сетевая система хранения данных Network Attached Storage

В РГАНТД используется как система Network Attached Storage для сетевого хранения данных, так и файловые серверы (Приложение 3).

В связи с использованием в РГАНТД серверов и компьютеров под ОС Windows и Linux должен решаться вопрос о совместном использовании накопленной информации. С этой целью был использован специальный компьютер предоставляющий совместный доступ разным операционным системам. Для решения задачи был установлен готовый NAS (Network Attached Storage) сервер компании QNAP – Quality Network Appliance Provider модель Q809U.

Основные преимущества использования NAS-устройств:

- простота инсталляции и обслуживания;
- относительно низкая цена и стоимость владения;
- возможность доступа к данным при отключенном основном сервере;
- обслуживание клиентов, работающих с различными ОС;
- бесплатное обновление ПО.

NAS-серверы – сетевые устройства хранения данных, не зависящие от операционных систем. Эта архитектура позволяет напрямую подключать устройства хранения данных к сети (т.е. фактически к концентратору, без участия сервера или ПК), встраивать непосредственно в них поддержку сетевых протоколов (например, TCP/IP), а также использовать их в специальных приложениях (например, для хранения и передачи видеоизображения).

NAS-устройства не являются полноценными серверами, они выполняют одну специализированную задачу – диспетчеризацию файлов – и ни для каких других целей не применимы. Благодаря архитектуре операционной системы Linux, которая позволяет расширять функциональность без особых проблем, в современных системах NAS присутствуют такие функции как сервер печати, web-сервер, серверы DLNA и iTunes. В состав NAS-серверов входит только самое необходимое – им не нужны клавиатуры, мыши, мониторы, порты ввода-вывода. К самому NAS-серверу можно подключить несколько дополнительных устройств хранения. Так что суммарный объем информации может составлять несколько сотен терабайт. Каждый NAS-сервер соединяется с накопителями по схеме «точка—точка» и взаимодействует с локальной сетью посредством стандартных сетевых протоколов, полностью контролируя передачу данных между подключенными к нему устройствами хранения и другими узлами сети.

Применение NAS-серверов позволяет уменьшить загрузку основного сервера, сняв с него обязанность непосредственной работы с файлами.

Некоторые модели серверов поставляются с предустановленными дисками, для других возможность выбора дисков предоставлена пользователю.

Возможности систем NAS достаточно однотипны, однако когда доходит до выбора дисков, производители разделяются на два противоположных лагеря. Одни предлагают готовые устройства с предустановленными дисками

и готовые к работе сразу после покупки. Другие – модели, для которых выбор дисков остаётся за пользователем. В таком случае можно заранее подумать о том, что требуется от диска (наряду с ёмкостью). В общем случае экономичность должна цениться выше, чем производительность. В большинстве случаев "узким местом" в производительности являются не диски, а сама система NAS, процессор RAID. Даже при чтении диски на 7200 об/мин не показывают преимуществ.

Все сегодняшние системы NAS для настройки используют Web-интерфейс. Можно выбрать один из следующих уровней RAID: 0, 1, 5 или 6 в зависимости от того, что важнее (скорость, сохранность данных или и то и другое). Можно настроить и другие возможности, которые выходят за рамки предоставления общего доступа по протоколу SMB.

Функциональность медиасервера включает поддержку показа фото и воспроизведения аудио и видео файлов через Web-интерфейс. Кроме того, имеется встроенный сервер DLNA (Digital Living Network Alliance), который обеспечивает потоковое вещание мультимедиа контента с NAS на совместимые с DLNA устройства в сети. Большинство сегодняшних NAS могут работать с данными по протоколам http, https, ftp и BitTorrent.

При приобретении системы NAS без предустановленных дисков или при обновлении дисков существующего сервера NAS нужно хорошо понимать, какие диски лучше подойдут для их целей. Возможности выбора дисков определённой ёмкости достаточно широки во всём диапазоне от 160 Гбайт до 2 Тбайт. Однако, с учётом постоянного роста цен на электроэнергию, имеет смысл учитывать энергопотребление дисков при выборе моделей, особенно, если планируется установить их в систему NAS. Также чем ниже энергопотребление, тем меньше тепловыделение.

Увеличение скорости чтения не является единственным преимуществом установки экономичных дисков. Снижается энергопотребление системы в целом, поскольку диски 5400 об/мин потребляют меньше энергии, чем модели

на 7200 об/мин. Кроме того, поскольку экономичные диски выделяют меньше тепла, NAS будет работать тише, поскольку вентиляторы будут работать с меньшей нагрузкой, также процесс загрузки будет сопровождаться меньшим уровнем шума.

Перед приобретением дисков, следует убедиться, что система NAS поддерживает выбранные модели, так как не все модели дисков, независимо от скорости вращения, могут быть совместимы с выбранной системой NAS. Также могут поддерживаться не все функции дисков. Если, например спящий режим жёсткого диска не поддерживается, то диски никогда не будут останавливаться, и о преимуществе в энергопотреблении экономичных моделей можно забыть.

3. Применяемость «облачных» технологий при организации хранения и использования электронных документов

Рекомендации по использованию «облачных» технологий при создании хранилища электронных документов единого центра хранения электронных документов в сфере организации государственного архивного хранения базируются на создании информационной системы хранения электронных документов на основе моделей обслуживания «Soft as a Services» (SaaS)[3], «Infrastructure as a Service» (IaaS)[4] , «Platform as a Service» (PaaS)[5].

«Облачные» технологии (cloud computing) или как их называют, вычисления, являются перспективным направлением в современных информационных технологиях.

Государственная программа «Информационное общество (2011-2020 годы)», утвержденная Распоряжением Правительства Российской Федерации от 20 октября 2010 г. № 1815-р, в подпрограмме «Электронное государство и эффективность государственного управления» характеризует развитие

---

[3] Программное обеспечение как услуга (SaaS) – модель, в которой потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств или посредством тонкого клиента, например, из браузера (например, веб-почта) или интерфейс программы. Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, операционных систем, хранения, или даже индивидуальных возможностей приложения (за исключением ограниченного набора пользовательских настроек конфигурации приложения) осуществляется облачным провайдером.

.

[4] Инфраструктура как услуга (IaaS) – модель предоставляется как возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетей и другими фундаментальными вычислительными ресурсами, например, потребитель может устанавливать и запускать произвольное программное обеспечение, которое может включать в себя операционные системы, платформенное и прикладное программное обеспечение. Потребитель может контролировать операционные системы, виртуальные системы хранения данных и установленные приложения, а также ограниченный контроль набора доступных сервисов (например, межсетевой экран, DNS). Контроль и управление основной физической и виртуальной инфраструктурой облака, в том числе сети, серверов, типов используемых операционных систем, систем хранения осуществляется облачным провайдером.

.

[5] Платформа как услуга (PaaS) – модель определяет предоставление потребителю возможности размещения в облачной инфраструктуре программного обеспечения, созданного потребителем на базе (платформе) инструментальных средств, предоставляемых облачным провайдером. При этом контроль и управление инфраструктурой облака осуществляется провайдером., а пользователь управляет своими приложениями.

«облачных» вычислений к числу приоритетных задач до 2015 года. Мероприятия программы направлены на создание национальной платформы «облачных» вычислений, в том числе:

- Разработка интернет-платформы «облачных» технологий, обеспечивающей безопасную работу с типовыми программными приложениями в режиме «программное обеспечение как услуга».
- Разработка на базе национальной программной платформы набора типовых программных сервисов для использования в органах государственной власти, включая средства коллективной работы с документами, общедоступное сетевое хранилище данных, средства удаленного хостинга программных приложений, средства разработки программного обеспечения.
- Интеграция национальных сетевых программных сервисов с крупнейшими коммерческими ресурсами, предоставляющими программное обеспечение в режиме услуги.

3.1. Общие рекомендации по применению «облачных» компонент

Модели обслуживания целесообразно выбирать на стадии разработки технического задания таким образом, чтобы не было разрыва между прикладной частью и инфраструктурой.

Выбор модели развертывания определяется поставленными целями. Рекомендуется использовать такую модель развертывания как частное облако (Private Cloud). При данной модели развертывания управление и эксплуатация системы осуществляется для различных потребителей объединенных единой инфраструктурой в одной организации. В отличии, например, от модели развертывания публичное облако (Public Cloud), при которой инфраструктура доступна для широкого использования в рамках нескольких организаций.

В целях повышения эффективности работы и экономии средств рекомендуется приобретать работы и услуги по разработке и внедрению системы хранения данных в составе комплексного сервиса, включающего несколько связанных функционалов, в том числе:

- сервисы, обеспечивающие требуемую функциональность по модели SaaS;
- проведение работ по обеспечению информационной безопасности[6]

Рекомендуется использовать модель «Инфраструктура как услуга» для создания:

- системы архивного хранения и предоставления доступа к описаниям и электронных документов и электронным документам государственного архивного хранения в хранилище ЦХЭД.
- программного обеспечения, использующее специализированное системное программное обеспечение и имеющее специальные требования к аппаратной платформе.

Рекомендуется использовать модель «Платформа как услуга» для создания следующих компонент:

- Системы архивного хранения и предоставления доступа к электронным документам и цифровым копиям архивных документов.
- Хранилища данных информационных систем федеральных архивов, включая средства проверки на достоверность данных и передачи их в хранилище данных ЦХЭД.
- Средства взаимодействия с СЭД ФОИВ.
- Взаимодействия с системой идентификации электронной цифровой подписи.

[6] В соответствии с требованиями 152-ФЗ по защите персональных данных.

- Система обеспечения информационной безопасности.
- Сервисы взаимодействия с системой межведомственного электронного взаимодействия, инфраструктурой выдачи и обслуживания универсальных электронных карт, единым порталом государственных и муниципальных услуг, региональным порталом государственных и муниципальных услуг и иными системами, создаваемыми в рамках инфраструктуры электронного правительства.
- Сервисы взаимодействия с внешними информационными системами.

В тоже время идеологически нецелесообразно разделять систему по горизонтальному принципу. Это может привести к ухудшению управляемости, безопасности и производительности. Возможно применение решений на основе секционирования по вертикальному принципу – секционирования на несколько центров обработки данных с возможной интеграции на прикладном уровне.

Для информационных систем, разработанных для использования в «облачной» инфраструктуре, необходимо обеспечить следующие характеристики:

- Открытая сервисно-ориентированная архитектура для использования программного обеспечения от различных поставщиков.
- Возможность единой точки доступа к электронным документам различных организаций.

Программное обеспечение по модели SaaS рекомендуется оснащать встроенными инструментальными средствами для изменения пользователем регламентов процессов, экранных форм, прав пользователей, отчетных форм и т.д.

Рекомендуется применять кроссплатформенное и промышленное программное обеспечение.

Разработку рекомендуется осуществлять на платформо-независимом языке программирования.

Первичная проверка корректности ввода информации и обязательности заполнения полей должна происходить без физического обращения на сервер (например, при помощи сценариев JavaScript) с целью снижения требований к каналам связи.

При работе с Public провайдерами (компании «Dropbox», «SkyDrive», «Google Drive», «Яндекс.Диск» и др.) необходимо развертывание на их ресурсах Private сервисов.

В будущим возможно использовать услуги государственного проекта по созданию Национальной облачной платформы (Проект «О7»). Проект реализуется компанией ОАО «Ростелеком». Задачи проекта Национальная облачная платформа – разместить в «облаке» электронное правительство, муниципалитеты, электронный документооборот и т.д. Проект базируется на модели IaaS и наборе SaaS сервисов (Приложение 6).

3.2. «Облачное» хранилище данных

«Облачное» хранилище данных представляет собой онлайн-хранилище, в котором данные хранятся на многочисленных, распределённых в сети серверах, предоставляемых в пользование клиентам.

В противовес модели хранения данных на собственных, выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту, в общем случае, не видна. Данные хранятся, а равно и обрабатываются, в облаке, которое представляет собой, с точки зрения клиента, один большой, виртуальный сервер. Физически же такие серверы могут располагаться удалённо друг от друга географически, вплоть до расположения на разных континентах.

Преимущества «облачных» хранилищ:

- Клиент платит только за то место в хранилище, которое фактически использует, но не за аренду сервера, все ресурсы которого он может и не использовать.
- Клиенту нет необходимости заниматься приобретением, поддержкой и обслуживанием собственной инфраструктуры по хранению данных, что, в конечном счете, уменьшает общие издержки производства.
- Все процедуры по резервированию и сохранению целостности данных производятся провайдером «облачного» центра, который не вовлекает в этот процесс клиента.

Потенциальные вопросы:

- Безопасность при хранении и пересылке данных является одним из самых основных вопросов при работе с облаком, особенно в отношении конфиденциальных, приватных данных.
- Общая производительность при работе с данными в облаке может быть ниже таковой при работе с локальными копиями данных.
- Надежность и своевременность получения и доступности данных в облаке очень сильно зависит от многих промежуточных параметров, в основном, таких как каналы передачи данных на пути от клиента к облаку, вопрос последней мили, вопрос о надлежащем качестве работы интернет-провайдера клиента, вопрос о доступности самого облака в данный момент времени.

3.3. Рекомендации по взаимодействию с внешними системами

Система взаимодействия ЦХЭД и СЭД ФОИВ осуществляет взаимодействие по типовым технологиям типа FTP[7] или «точка-точка» на основе протоколов межведомственного электронного взаимодействия

[7] File Transfer Protocol

(СМЭВ), систем электронного документооборота (СЭДО). Это определяет состав и технические требованиям к сетевому телекоммуникационному оборудованию федеральных архивов для возможного применения «облачных» технологий.

4. Хранилище электронных документов

Хранилище электронных документов – это программно-аппаратный комплекс, обеспечивающий структурированное хранение документов в электронном виде.

Хранилище электронных документов также включает в себя управление документами, обеспечивает миграцию электронных документов с одного носителя на другой, обеспечивает целостность данных.

Хранилище документов может представлять собой как файловое хранилище, так и хранилище в виде СУБД или Document management system[8] (DMS). В свою очередь, хранилище документов в СУБД может производиться как в одной (единой) базе данных, так и в раздельных базах данных.

Наиболее перспективным оценивается направление систем предоставляемых по модели обслуживания SaaS. Использование модели обслуживания SaaS должно сопровождаться жесткими требованиями соглашения об уровне предоставления услуг SLA (Service Level Agreement) и требованиям обеспечивающим информационную безопасность.

Метаданные хранятся для каждого документа. Метаданные, например, могут включать дату занесения документа в хранилище и идентификатор пользователя, совершившего это действие. Система управления документами (например, Document management system) также может извлекать метаданные из документа автоматически или запрашивать их у пользователя. Поисковая система хранилища электронных документов должна предоставлять по индексированию текста электронных документов или использовать индексы, имеющиеся у электронных документов для информационного поиска документа.

[8] набор компьютерных программ, используемых для отслеживания и хранения электронных документов и/или образов бумажных документов

4.1. Аппаратные и программные платформы для хранения массивов электронных документов

Хранение характеризуется двумя основными параметрами: емкость хранилища данных и скорость предоставления данных (отклик на запрос), а также степенью резервирования и дублирования, масштабируемостью систем хранения.

Существует несколько способов увеличения емкости хранения данных:

1. Установка дополнительных жестких дисков.
2. Установка дополнительного файлового сервера или системы хранения данных (СХД).
3. Использование ленточных и магнитооптических устройств для архивации информации.

Дополнительные жесткие диски. Установка в файловый сервер новых накопителей на жестких дисках, не требующих остановки работы сервера и проведение специальных настроек сервера и дисковой системы.

Дополнительный файловый сервер. С технологической точки зрения установка дополнительного файлового сервера достаточно эффективна, т.к. при этом достигается максимальное повышение скорости передачи данных и рост количества одновременно обрабатываемых запросов.

При резервном копировании данных (для восстановления функционирования сети в случае сбоя) объемы сохраняемых файлов (архивных электронных документов) постоянно растут и хранить на дисках файлового сервера такие объемы данных достаточно дорого.

Ленточные или магнитооптические (МО) накопители. Эти устройства применяют для удешевления системы хранения резервной или редко

используемой информации. Для хранилищ большого объема данных (архивного хранения электронных документов) целесообразно применять системы хранения, оснащенные автозагрузчиками. Автозагрузчики являются устройствами со сменными носителями информации, благодаря чему могут хранить достаточно большой (от сотен гигабайт) объем данных. Автозагрузчик состоит из отсеков (до десяти), в которых хранятся картриджи, и роботизированного механизма смены картриджей в дисководах (их, как правило, не больше двух). Применение таких накопителей значительно уменьшает объем рутинной работы по замене носителей, например, 8-секционный автозагрузчик позволяет копировать резервные данные понедельника на первый картридж, вторника – на второй и т. д. При этом картриджи не нужно менять каждый день (максимум раз в неделю). Автозагрузчики отличаются большими объемами хранимой информации и высокой скоростью предоставления информации, а также возможностью одновременно обслуживать большее количество запросов.

Перспективным является применение иерархических систем хранения, сочетающие в себе дисковые и ленточные подсистемы и имеющие автоматические механизмы перемещения данных между ними на основе частоты доступа.

Сетевые устройства хранения данных (Network-Attached Storage). Эффективным представляется подход к организации системы хранения данных на платформе NAS-сервера (Network-Attached Storage). NAS-серверы занимают «золотую середину» в современной «линейке» схем хранения данных и «облачных» хранилищ.

NAS-серверы – сетевые устройства хранения данных, не зависящие от операционных систем. Эта архитектура позволяет напрямую подключать устройства хранения данных к сети (фактически к концентратору, без участия сервера или ПК), встраивать непосредственно в них поддержку сетевых

протоколов (например, TCP/IP), а также использовать их в специальных приложениях (например, для хранения и передачи видеоизображения).

NAS-устройства практически выполняют одну специализированную задачу – диспетчеризацию файлов. Несомненным достоинством NAS-устройств является то, что они обеспечивают доступ к файлам даже при отключенном основном сервере.

К NAS-серверу можно подключить несколько дополнительных устройств хранения. Так что суммарный объем информации может составить от несколько сотен гигабайт до сотен терабайт.

Каждый NAS-сервер соединяется с накопителями по схеме «точка—точка» и взаимодействует с локальной сетью посредством стандартных сетевых протоколов, полностью контролируя передачу данных между подключенными к нему устройствами хранения и другими узлами сети.

Применение NAS-серверов позволяет уменьшить загрузку основного сервера, сняв с него рутинную обязанность непосредственной работы с файлами.

В РГАНТД для организации хранения данных используются технология NAS-сервер, сетевое хранение данных, файловые сервера.

Для хранения сверхбольших объемов данных перспективным представляется использование многоузловых комплексов с высокоскоростными соединениями между ними. Такие комплексы достаточно хорошо масштабируются и и обеспечивают лучшую производительность за счет организации параллельной работы.

Критерии выбор хранилищ данных

Основные критерии, по которым могут выбираться хранилища:

1. Доступный объем дискового пространства.
2. Кросс-платформенность.

3. Совместный доступ к файлам.

4.2. Характеристики хранилища электронных документов

Хранилище электронных документов ЦХЭД должно обеспечивать:

- сохранность электронных данных в течение длительного времени;
- возможность хранения больших объемов данных;
- исключение физической возможности удалить или изменить данные;
- энергонезависимость хранилища;
- интеграция с внешними информационными системами (системы документооборота, управления электронным архивом);
- возможности вирусо-, помехо- и катастрофоустойчивость;
- оперативный доступ к электронным документам в хранилище;
- оперативный кэш на жестких дисках, обеспечивающий возможность организации архива неограниченного объема за счет использования «горячей» замены носителей (off-line хранение) при централизованном управлении или системы с несколькими уровнями кэширования;
- наполнение, постоянное пополнение и актуализацию электронных информационных ресурсов;
- обеспечение аутентичности данных, при любых операциях управления документами над ними;
- простую интеграцию хранилища с важнейшими ведомственными информационными системами;
- возможность восстановления данных и документов на любую дату;
- возможность поиска документов по старым реквизитам и наименованиям (исторический поиск);

- функционирование защищенного хранилища документов и данных как единого источника информации, документов и знаний организации;
- соответствие электронных документальных фондов организации и их регистрационных данных требованиям законодательства;
- соответствие требованиям безопасности. (Приложение 4).

4.3. Структура хранилища электронных документов

1. Технические компоненты.

1. Серверный комплекс.
2. Система хранения данных и резервного копирования.
3. Состоит из консолидирующих дисковых массивов, сети хранения данных, системы резервного копирования и аварийного восстановления данных.
4. Сетевая инфраструктура обеспечивает взаимодействие между серверами, объединяет логические уровни и организует каналы связи. Включает магистрали для связи с операторами общего доступа, телекоммуникации, обеспечивающие связь пользователей с ЦОД.
5. Инженерная система эксплуатации.
6. Система безопасности для предотвращения несанкционированного вторжения в зоны конфиденциальной информации.

2. Программные компоненты.

- Системное программное обеспечение.
- Программное обеспечение баз данных.

- Операционные системы рабочих станций.
- Средства резервного копирования.
- Программное обеспечение устройств хранения данных.
- Средства администрирования серверов и рабочих станций.

5. Общие рекомендации по производительности и отказоустойчивости

Рекомендации по производительности и отказоустойчивости определяются исходя из положений “Требования к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающие, в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения”.

Работы по обеспечению информационной безопасности при обработке персональных рекомендуется выполнять в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных» (приказ ФСТЭК от 5 февраля 2010 г. № 58), «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Утверждена ФСТЭК России 14 февраля 2008 г.), «Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена ФСТЭК[9] России 15 февраля 2008 г.)

[9] Федеральная служба по техническому и экспортному контролю

6. Общие рекомендации по уровню подготовки персонала

Рекомендации по уровню подготовки специалистов, обслуживающих элементы Системы определяются нормативно-технической документацией на систему. Рекомендуется владение навыками в следующих дисциплинах:

- программные средства и платформы инфраструктуры информационных технологий учреждений;
- основы современных систем управления базами данных;
- основы информационной безопасности;
- основы программирования;
- языки современных бизнес-приложений;
- основы современных операционных систем;
- современные стандарты информационного взаимодействия систем;
- отраслевая нормативная техническая документация.

7. Системно-техническая инфраструктура хранения электронных документов

7.1. Общие положения

Система хранения электронных документов (хранилище) предназначена для обеспечения функционирования компонентов хранилища с необходимыми уровнями производительности, доступности и безопасности, а также для обеспечения катастрофоустойчивости компонентов на случай локальных катастроф.

Проектные решения система хранения электронных документов должны соответствовать ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение».

При вводе системы в эксплуатацию, а также в ходе эксплуатации, работы по настройке и испытанию должны проводиться квалифицированным обученным персоналом с соблюдением требований техники безопасности и в соответствии с эксплуатационной документацией на систему.

При производстве строительно-монтажных работ должны выполняться требования СНиП 12-03-2001 «Безопасность труда в строительстве. Часть 1. Общие требования», СНиП 12-04-2002 «Безопасность труда в строительстве. Часть 2. Строительное производство», соответствующих санитарно-технических норм и правил, а также других нормативных документов.

Показатели по обеспечению безопасности при монтаже, эксплуатации, обслуживании и ремонте технических средств должны соответствовать требованиям ГОСТ 12.2.003-91.

При производстве строительно-монтажных, пусконаладочных работ необходимо руководствоваться требованиями «Правил пожарной безопасности в Российской Федерации» ППБ 01-03.

Решения по выбору оборудования и его размещению в рамках проекта соответствуют требованиям СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы», а также требованиям к помещениям для работы с ПЭВМ, микроклимату, содержанию аэроионов и вредных химических веществ в воздухе на рабочих местах, оборудованных ПЭВМ, уровням шума и вибрации на рабочих местах, освещению на рабочих местах, инфракрасному, ультрафиолетовому, рентгеновскому и электромагнитному излучениям, уровням электромагнитных полей на рабочих местах, визуальным параметрам ВДТ, контролируемым на рабочих местах. Допустимые электромагнитные поля радиочастот на рабочих местах соответствуют ГОСТ 12.1.006-84.

При проектировании должен использоваться передовой опыт основных мировых организаций-лидеров в области информационных технологий: IBM, Oracle, HP, EMC, Symantec и VMware.

Представляется методически правильным создание удаленного хранилища данных (удаленной площадки), объединённой с основным хранилищем данных (с основной площадкой) каналами связи. Такой подход позволяет решить проблему катастрофоустойчивости.

Эксплуатационные характеристики системы хранения электронных документов:

- Производительность – измеряемая как количество обрабатываемых данных за определенное время или как среднее время отклика системы (без учета задержки вносимой передачей данных по линям связи) при одновременной работе определенного количества пользователей.
- Максимальное количество обрабатываемых информационных объектов (максимальный объем базы данных).

- Требования к надежности, выражаемые доступностью (коэффициент или суммарно допустимое время простоя за год) и максимально допустимое время однократного простоя системы.

Для обеспечения надежного функционирования хранилища электронных документов необходимо выполнение следующих условий:

- Поддержание программно-технической инфраструктуры в работоспособном и непрерывном состоянии.
- Обеспечение целостности, доступности и конфиденциальности информации.
- Резервирование и восстановление работы системы и ее отдельных программно-технических компонент.
- Поддержка технической и эксплуатационной документации в актуальном состоянии.

С этой целью необходимо разработать перечень программно-технических компонент, которые бы обеспечивали выполнение данных условий.

Обслуживание программно-технического комплекса хранилища электронных документов должно осуществляться специалистами по эксплуатации в соответствии с разработанными требованиями к режиму эксплуатации: в течение 7 дней в неделю, 24 часа в сутки (функционирования по схеме «24x7x365» – 24 часа в сутки, 7 дней в неделю круглогодично).

Необходимым условием является проведение регламентных и профилактических работ, а также контроль над соблюдением эксплуатационных требований.

7.2. Рекомендации по основным техническим решениям

Рекомендации по основным техническим решениям создания хранилища электронных документов распространяются на решения по структуре системы и подсистемам, а также способам информационного обмена между компонентами системы.

С этой целью можно рекомендовать создание компонентной модели для проектирования системы хранения, например, на стадии эскизного проектирования.

Системно-техническая инфраструктура хранилища электронных документов (СТИ ХЭД) – совокупность программных и аппаратных средств, основной задачей функционирования, которых является обеспечение необходимых вычислительных ресурсов для надежного и бесперебойного функционирования хранилища электронных документов.

Пользователи подключаются к системе хранения данных через ЦХЭД. Системно-техническая инфраструктура хранилища электронных документов должна также включать подсистему обеспечения информационной безопасности.

Решения по системно-технической инфраструктуре хранилища.

Системно-техническая инфраструктура хранилища электронных документов представляет собой совокупность следующих подсистем и компонентов:

- подсистема приема и обработки данных;
- подсистема хранения данных;
- подсистема резервного копирования;
- подсистема инфраструктурных сервисов;
- подсистема управления и мониторинга;

- локальная вычислительная сеть (ЛВС);
- сеть хранения данных (SAN);
- подсистема передачи данных;
- подсистема обеспечения информационной безопасности;
- инженерная подсистема.

Решения по взаимосвязям и совместимости основной и удаленной площадками.

Взаимодействие между основной и удаленной площадкой осуществляется за счет осуществления взаимодействия между подсистемами обработки при реализации возможного режима Parallel Sysplex и реализации репликации данных в соответствии с требованиями по надежности функционирования систем при авариях и распределенного функционирования.

Совместимость функционирования подсистем основной и удаленной площадок обеспечивается использованием следующих принципов:

1. Использование единообразной архитектуры площадок.
2. Использование идентичного или полностью аналогичного оборудования и конфигурации данного оборудования.

Решения по режимам функционирования системы.

Решение по режимам функционирования системы СТИ ХЭД определяет функционирование в следующих режимах:

- штатный режим – основной режим функционирования;
- восстановления работоспособности технических и программных средств (от момента аварии до восстановления штатного режима) (соответствует недоступности системы);

- профилактический режим в соответствии с регламентом.

В штатном режиме СТИ ХЭД должна обеспечивать полную производительность всех систем хранилища данных.

В режиме «после аварии» необходимо перед запуском штатного режима необходимо предварительное тестирование программно-технических компонент.

Время нахождения в режиме «восстановления работоспособности ИУС» определяется в соответствии с регламентом функционирования хранилища электронных документов и не должно превышать значений, указанных в требованиях к системам ЭДО ФОИВ.

В профилактическом режиме допускаются в запланированное время ограничения к доступу к системе или к отдельным компонентам системы в соответствие с регламентом, который должен быть разработан в процессе рабочего проектирования.

Решения по численности, квалификации и функциям персонала системы, режимам его работы и порядку взаимодействия

Решения по численности персонала, его квалификации, а также по его функциям, должны соответствовать требованиям к квалификации обслуживающего персонала и режиму его работы. Должны быть подготовлены предложения по составу курсов обучения персонала, сертификации фирмами-производителями технических средств и системного программного обеспечения.

Специалисты эксплуатирующей организации обеспечивают поддержание технических и программных средств в работоспособном состоянии во всех режимах функционирования, выполняют периодическое обслуживание, обеспечивают выполнение ремонтных работ, осуществляют резервное копирование, архивирование и восстановление данных,

осуществляют администрирование (настройку, конфигурирование, поддержку) технических, программных средств и прав доступа, осуществляют загрузку, контроль и исправление данных, ведение справочников и классификаторов данных.

С целью обеспечения эффективного функционирования аппаратно-программных средств СТИ ХЭД обслуживающий персонал обеспечивает решение следующих задач:

- техническое обслуживание;
- администрирование;
- конфигурирование;
- развитие системы (включая соединение с подсистемами и внешними системами);
- восстановление данных и программного обеспечения.

Для обслуживания комплекса технических и программных средств СТИ ХЭД необходимо предусмотреть следующие категории специалистов:

- специалист по обслуживанию комплекса технических средств СТИ ХЭД, обеспечивающий обслуживание серверного и сетевого оборудования (с учетом специализаций по видам оборудования);
- администратор СУБД, обеспечивающий работоспособность СУБД и технологическую поддержку сохранности баз данных;
- специалист сменного персонала по мониторингу комплекса технических средств, обеспечивающий обслуживание и мониторинг (с учетом специализаций по видам оборудования).

Специализации специалистов по обслуживанию комплекса технических средств:

- Администраторы СУБД.

- Администратор серверного оборудования.
- Администраторы сетевого оборудования в части сетей хранения данных.
- Администраторы сетевого оборудования в части подсистемы резервного копирования.
- Администраторы сетевого оборудования в части подсистемы хранения данных.
- Администраторы мониторинга и управления сетевого оборудования в части подсистемы.

Основные функции персонала служб эксплуатации приведены в таблице 7.1.

Таблица 7.1

Функции персонала служб эксплуатации

Категория	*Функции*
Специалист по обслуживанию КТС	Поддержка системного программного обеспечения и оборудования СТИ ХЭД в работоспособном состоянии. Восстановление системы в случае нарушений работоспособности оборудования Настройка и оперативное изменение конфигурационных параметров системного программного обеспечения и оборудования СТИ ХЭД. Мониторинг работы СТИ ХЭД. Просмотр системного журнала.
Администратор СУБД	Поддержание СУБД на серверах СТИ ХЭД в работоспособном состоянии. Восстановление СУБД в случае нарушений ее работоспособности.

Категория	*Функции*
	Настройка и оперативное изменение конфигурационных параметров СУБД Просмотр системного журнала СУБД.
Сменный персонал	Круглосуточный мониторинг работоспособности СТИ ХЭД.

Согласно общим требованиям к надежности системы уровень надежности зависит от уровня квалификации персонала, организации работ и уровня надежности действий персонала. Таблица 7.2 отражает требования к квалификации персонала.

Таблица 7.2

Требования к квалификации обслуживающего персонала

Категория	*Требования к квалификации*
Специалист по обслуживанию комплекса технических средств	Опыт администрирования системного программного обеспечения, серверного и другого оборудования от трех лет
Администратор СУБД	Опыт администрирования СУБД от трех лет.
Сменный персонал	Опыт администрирования системного ПО, серверного и другого оборудования КТС от одного года

Эксплуатирующий персонал обеспечивает поддержание комплекса технических средств в работоспособном состоянии во всех режимах функционирования, а также выполняет периодическое обслуживание и ремонтные работы. При этом режим работы эксплуатационного персонала

должен соответствовать графикам работы согласно штатному расписанию эксплуатирующей организации.

Решения по обеспечению характеристик системы хранения электронных документов

Обеспечение рабочих характеристик определяется объемом оперативной памяти, объемом дискового пространства и вычислительной мощностью программно-аппаратных платформ, необходимых для обеспечения штатного режима работы.

Для обеспечения рабочих характеристик необходимо отслеживать нагрузку на основные подсистемы, выявлять узкие места и, в случае необходимости, принимать меры к их устранению.

7.3. Обеспечение общих требований к надежности

Для обеспечения показателей надежности при проектировании СТИ ХЭД должны использоваться следующие методы обеспечения надежности:

- выбор ремонтопригодных технических средств, с высокими показателями безотказности;
- резервирование, дублирование компонентов системы;
- дублирование подключений критически важных компонентов к активному сетевому оборудованию;
- кластерные технологии;
- обеспечение сохранности данных и ПО;
- обеспечение требуемых условий эксплуатации;
- ведение статистического учета аварийных ситуаций;
- обеспечение бесперебойного электроснабжения технических средств.

Методы резервирования компонентов системы:

- резервирование серверного оборудования подсистемы обработки, подсистемы мониторинга и управления, подсистемы резервного копирования, службы доступа пользователей;
- внутреннее резервирование компонентов дискового массива подсистемы хранения данных;
- внутреннее резервирование компонентов ленточной библиотеки подсистемы резервного хранения;
- дублирование коммуникационного оборудования.

Для повышения надежности работы оборудования рекомендуется использование механизмов внутреннего резервирования:

- внутренних дисковых RAID-массивов уровня 1 (зеркалирование) и уровня 5 (параллельная работа) для серверного оборудования и дисковых массивов;
- дополнительных блоков питания и вентиляторов с поддержкой «горячей» замены для серверного оборудования, дисковых массивов, ленточных библиотек, коммуникационного оборудования;
- дублирование контроллеров для дисковых массивов и ленточной библиотеки;
- резервирование ленточных приводов в ленточных библиотеках.

В течение срока службы технических средств допускается замена узлов, плат и отдельных блоков в случае их выхода из строя или в соответствии с требованиями эксплуатационной документации.

Для обеспечения необходимого качества и безопасности программного обеспечения рекомендуется:

- в качестве программного обеспечения использовать только лицензионное ПО с действующей технической поддержкой от фирм-производителей;
- компоненты ПО не должны нарушать целостности друг друга;
- необходимо предусмотрено обеспечение целостности информации в базах данных и программного обеспечения СТИ ХЭД в случае отказов и сбоев в работе программно-технических средств, в том числе отключение питания.

При авариях сохранность информации средствами СТИ ХЭД обеспечивается доступность следующих данных, хранимых на серверах и системах хранения:

- прикладные данные;
- системные данные:
- системное программное обеспечение и конфигурационные наборы данных;
- программное обеспечение, таблицы, конфигурационные файлы и журналы систем управления базами данных (СУБД);
- журналы изменений Системы и активности пользователей.

В проектных решениях должна быть предусмотрена минимизация потери информации в случае отказа компонентов СТИ ХЭД по следующим причинам:

- повреждение электропитания;
- выход из строя микропроцессорного оборудования;
- повреждение кабельной системы;
- физическое повреждение носителей информации, находящихся в эксплуатации;

- злоумышленные действия.

Сохранность информации в этих случаях обеспечивается за счет:

- централизованного хранения информации на отказоустойчивом оборудовании подсистем хранения данных и резервного копирования и восстановления данных СТИ ХЭД;
- реализации принципа избыточности хранения информации;
- программных решений по обеспечению целостности баз данных при сбоях в проведении транзакций;
- организации бесперебойного электропитания серверов.

Комплекс мер по обеспечению сохранности информации и ее восстановления с соблюдением ограничений на время однократного простоя системы включает в себя:

- проведение регулярного регламентного копирования базы данных;
- проведение внепланового резервного копирования базы данных;
- хранение резервных копий в разных помещениях с техническими средствами (серверами, активным сетевым оборудованием и т.п.);
- восстановление базы данных из резервных копий;
- исключение несанкционированного доступа к резервным копиям;
- автоматическое обнаружение сбоя любого из устройств, включая автоматизированную диагностику причин сбоя.

Резервное копирование и восстановление данных с резервной копии должно осуществляться в соответствии с разработанным регламентом резервного копирования и восстановления данных.

7.4. Системный ландшафт и подсистемы

Системный ландшафт реализуется из трех систем:

- Система разработки и настройки (DEV).
- Система тестирования разработок (QAS);
- Система постоянной эксплуатации (PRD).

Решения по реализации функций подсистемы обработки данных.

Подсистема обработки данных обеспечивает выполнение следующих функций:

- предоставления системно-технической среды функционирования, тестирования и разработки информационно-управляющих систем за счет использования аппаратно-программных комплексов, совместимых с прикладным программным обеспечением информационно-управляющей системы;
- создание специальной (изолированной) среды для функционирования различных информационно-управляющих систем входящих в структуру хранилища электронных документов с возможностью динамического перераспределения ресурсов между ними за счет использования оборудования и системного программного обеспечения, поддерживающего виртуализацию ресурсов (например, Solaris Container, Resours Pool);
- управления функционированием технических средств и системного программного обеспечения посредством использования средств самодиагностики, администрирования и интеграции с подсистемой мониторинга и управления.

Используемое серверное оборудование должно обеспечивать, как «горизонтальное» (увеличение количества совместно функционирующих

средств), так и «вертикальное» (наращивание внутренних мощностей технических средств), а также возможности масштабирования, достаточные для обеспечения надежного функционирования.

Для этого на применяемых платформах должна быть задействована технология виртуализации, например:

Создание логических разделов типа LPAR (Logical Partition) на платформах IBM System z и IBM Power.

Применение аппаратных разделов Domain и виртуальных машин Solaris Container на платформе Sun SPARC.

Можно также рекомендовать выделение пулов ресурсов с общими виртуальными настройками соединений.

Решения по реализации функций подсистемы хранения данных

Подсистема хранения обеспечивает следующие функции:

- надежное хранение данных (раздел 7.3)
- отказоустойчивый, высокопроизводительный доступ серверов к устройствам хранения и репликации данных за счет построения подсистемы хранения данных на основе дисковых хранилищ, подключенных по выделенной сети хранения данных.

Обеспечиваются иерархические уровни хранения подсистемы хранения данных:

- уровень мгновенного доступа за счет использования дисков с интерфейсами внутри дисковых массивов (интерфейс FC).
- уровень текущего доступа за счет использования дисков с интерфейсами SATA или аналоги для мгновенных копий и других данных, требуемых эпизодически.

- уровень долгосрочного хранения данных (уровень отложенного доступа) – хранение данных, доступ к которым осуществляется редко, на кассетах ленточных библиотек (подсистема резервного копирования и восстановления данных).

Используемые программные и аппаратные средства должны позволять применить методы репликации данных между основным и резервным хранилищем данных и обеспечивать требования по информационной безопасности.

Решения по реализации функций подсистемы резервного копирования

Подсистема резервного копирования выполняет следующие функции:

- обеспечивает возможность восстановления данных при восстановлении систем после аварии или катастрофы при их логическом разрушении или другим причинам, не позволяющим восстановить функционирование систем с помощью реплицированных данных (данная функция обеспечивается за счет использования технических средств (ленточная библиотека, сервера резервного копирования) и программного обеспечения резервного копирования и восстановления, поддерживающего возможности восстановления данных из предыдущих состояний на определенный период времени);
- обеспечивает возможность сохранения на ленточных библиотеках всей информации, хранимой на серверах и дисковых массивах.

Аппаратно-программный комплекс подсистемы позволяет управлять резервным копированием и восстановлением данных как по расписанию (согласно регламенту), так и в ручном режиме, что обеспечивает возможность формирования копий данных с определенной регламентом резервного

копирования периодичностью, а также оперативных копий перед внесением изменений или по запросу.

Комплекс технических и программных средств подсистемы резервного копирования обеспечивает создание и выполнение заданий по расписанию, ведение журналов копирования, сохранение вместе с данными необходимых параметров и атрибутов.

Система резервного копирования должна поддерживать режимы полного, инкрементального и дифференциального копирования.

Решения по реализации функций подсистемы мониторинга и управления

Подсистема мониторинга и управления обеспечивает выполнение следующих функций:

- сбор информации о параметрах функционирования технических и программных средств;
- накопление информации о параметрах функционирования технических и программных и ее хранение с использованием собственных технических средств;
- представление информации о параметрах функционирования технических и программных в оперативном режиме с использованием графического интерфейса и развитых средств навигации;
- оперативно-техническое управление функционированием и администрирование технических и программных средств;
- формирование обобщенных показателей состояния функционирования технических и программных средств, как в целом, так и отдельных технических средств;

- выгрузка в оперативном и регламентном режимах по запросу групп собираемых параметров функционирования отдельных технических средств;
- распространение и установка программного обеспечения и обновлений;
- установка операционных систем;
- удаленное управление серверами.

Подсистема мониторинга и управления обеспечивает решение следующих задач:

- событийный контроль функционирования и предоставление данных процессам эксплуатации;
- мониторинг и управление ресурсов;
- распространение и установка обновлений для операционных систем.

Подсистема мониторинга и управления инфраструктурой функционально должна быть разделена на модули. Возможный модульный состав подсистемы приведен в таблице 7.3.

Решения по комплексу технических и программных средств (КТС)

В соответствии с требованиями к режимам функционирования должен быть установлен режим функционирования по схеме «24х7х365» (24 часа в сутки, 7 дней в неделю круглогодично).

Комплекс технических средств обеспечивает требуемую готовность, надежность функционирования и доступность данных. Для этого в составе комплекса реализуются возможности диагностики, резервирования и взаимозаменяемости аппаратных компонентов.

При выборе состава оборудования необходимо учитывать требование по обеспечению планируемого масштабирования производительности в

соответствии с возрастающим уровнем рабочей нагрузки, связанным с ростом потоков электронных документов принимаемых на хранение.

Таблица 7.3

Модули подсистемы мониторинга и управления

Модуль	*Назначение*
Модуль мониторинга и управления инфраструктурой хранения данных	Назначением модуля является автоматизация процессов управления емкостью ресурсов хранения, управления и контроля ресурсов хранения и дискового пространства на уровне устройств и логических томов (LUN), а также мониторинг и управление инфраструктурой сети хранения данных. Предназначен для персонала, эксплуатирующего инфраструктуру хранения данных.
Модуль мониторинга и управления сетевой инфраструктурой	Назначением модуля мониторинга и управления сетевой инфраструктурой является оперативное представление состояния функционирования сетевой инфраструктуры. Предназначен для персонала, эксплуатирующего сетевую инфраструктуру.

Модуль	*Назначение*
Модуль мониторинга и управления серверной и прикладной инфраструктурой	Назначением модуля является обеспечение мониторинга работоспособности и производительности серверного оборудования и ПО, а также оказание оперативного управляющего воздействия в случае необходимости. Модуль осуществляет функцию сбора и обработки информации о производительности и доступности программного обеспечения на уровне прикладных сервисов, в том числе, упреждающего обнаружения проблем, связанных с прикладными сервисами, контроля выполнения соглашений об уровне обслуживания, анализа и выявления причин сбоев, управления производительностью серверов и распределением нагрузки между ними. Предназначен для персонала, эксплуатирующего серверную и прикладную инфраструктуру.

Примерный (возможный) состав оборудования в составе комплекса технических средств:

Оборудование подсистемы обработки данных:

- сервер базы данных (например, сервер БД SAP IBM zEnterprise);
- серверы приложений (например, IBM Power 595);
- сервер служебный (например, IBM Power 570);

Коммуникационное оборудование сетей хранения данных:

- директоры сети хранения данных (например, IBM SAN768B).

Оборудование подсистемы хранения данных:

- дисковый массив хранения данных (например, IBM System Storage DS8300);

Оборудование подсистемы резервного копирования:

- ленточная библиотека (например, IBM System Storage TS3500 Tape Library).

Примерная (возможная) конфигурация сервера:

- центральный процессор Central Processor (CP7) (до 10 ед.);
- специализированный процессор Integrated Coupling Facility (ICF) (до 2 ед.);
- специализированный процессор Integrated Information Processor (zIIP) (до 7 ед.);
- память в объеме 256 ГБ;
- 8 портов InfiniBand IB-DDR 5 Гбит/с;
- плата 4-х портовая FICON Express8 SX (до 10 ед.);
- плата 4-х портовая Open Systems Adapter (OSA) Express3 1000Base-SX (до 2 ед.);
- плата 4-х портовая OSA Express3 1000Base-T (до 4 ед.);
- плата 2-х портовая OSA Express3 10GBase-SR (до 4 ед.).

Управление сервером должно осуществляться с помощью одной или двух консолей, выполненных на базе ПК со специализированным программным обеспечением.

Выделение ресурсов каждому разделу LPAR выполняется в соответствии с соблюдением того, что:

- каждый физический процессор должен быть разделяемым (shared). Это позволяет разделу использовать физические CP, когда система переходит в режим ожидания;
- требуемый объем оперативной памяти закреплен за каждым из разделов;

- запросы ввода-вывода обрабатываются динамически в соответствии с их приоритетами и требуемой производительностью.

Решения по организации высокой доступности

Решения по организации высокой доступности базируется на применение серверов, которые обладают несколькими уровнями отказоустойчивости и обнаружения ошибок. Благодаря внутренней избыточности сервер при сбое переносит нагрузку с аварийных компонентов на рабочие компоненты, предотвратив прекращение обслуживания конечного пользователя. При этом компоненты, давшие сбой, могут быть демонтированы и заменены на другие при активном процессоре без прерывания обслуживания.

Вероятность приведения к останову при ошибках аппаратуры снижается инженерной избыточностью всех ключевых компонентов, что позволяет избежать появления единой точки отказа. Сервер обеспечивается резервным оборудованием для всех критических компонентов.

Сервер обеспечен двойным электропитанием по независимым кабелям. При перебое одного из источников второй способен обеспечить энергией весь сервер. При этом благодаря устройству блоков питания сервер не остановится и при пропадании одной фазы питающей трехфазной сети.

При нарушениях в работе внешней электросети устойчивую работу сервера на время поддержит встроенная батарея питания и источник бесперебойного питания.

Для выполнения требований по катастрофоустойчивости и доступности приложений возможно использование системы «Geographically Dispersed Parallel Simplex /Peer to Peer Remote Copy (GDPS/PPRC)».

Данная система является разработкой компании IBM и может быть адаптируется под различные проектные решения. Технология Parallel Sysplex

позволяет, управляя логическими разделами и их ресурсами, добиться отсутствия единых точек отказа.

Возможно также применение системы «Metro Mirror».

Система выполняет следующие основные функции:

- выполнение всех действий по восстановлению в случае выхода из строя основного хранилища;
- выполнение операций по остановке копирования данных, для сохранения данных на вторичных дисковых устройствах;
- предоставление аналитических данных по состоянию системы.

7.5. Система защиты

Система защиты должна иметь пять уровней защиты данных:

1. Защита сервера.
2. Защита сети.
3. Защита приложения.
4. Защита производительности
5. Защита данных.

Для достижения предлагаемой системы защиты можно рекомендовать программное обеспечение «VMware vCenter Server Heartbeat».

7.6. Требования к ресурсам

Примерные требования к основным системно техническим ресурсам приведены в таблицах 7.4 – 7.9.

Таблица 7.4.

Требования к ресурсам и ПО основного и резервного сервера, базы данных мониторинга

Показатель	*Значение*
Центральный процессор	2 ядра
Оперативная память	Не менее 8 ГБ
НЖМД	Не менее 320 ГБ
Количество интерфейсов Ethernet	Не менее 2 штук, для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 штук, для отказоустойчивости
Операционная система	AIX 6.1
База данных	DB2 9.5
Средства отказоустойчивости	Veritas Cluster Server

Таблица 7.5

Требования к ресурсам и ПО сервера управления

Показатель	*Значение*
Центральный процессор	8 ядер
Оперативная память	Не менее 32 ГБ
НЖМД	Не менее 160 ГБ
Количество интерфейсов Ethernet	Не менее 2 ед., для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 ед., для отказоустойчивости

Показатель	*Значение*
Операционная система	MS Windows Server 2008 EE SP2 x64
СУБД	Microsoft SQL Server 2008 Enterprise SP1
Средства отказоустойчивости	VMWare HA

Таблица 7.6

Требования к ресурсам и ПО сервера распространения

Показатель	*Значение*
Центральный процессор	2 ядра
Оперативная память	Не менее 8 ГБ
НЖМД	Не менее 160 ГБ
Количество интерфейсов Ethernet	Не менее 2 ед., для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 ед., для отказоустойчивости
Операционная система	MS Windows Server 2008 EE SP2 x64
СУБД	Используется БД сервера CMS21
Средства отказоустойчивости	VMWare HA

Таблица 7.7

Требования к ресурсам и ПО сервера контроля версий

Показатель	*Значение*
Центральный процессор	1 ядро
Оперативная память	Не менее 4 ГБ
НЖМД	Не менее 160 ГБ
Количество интерфейсов Ethernet	Не менее 2ед., для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 ед., для отказоустойчивости
Операционная система	MS Windows Server 2008 EE SP2 x64
База данных	Используется БД сервера CMS21
Средства отказоустойчивости	VMWare HA

Таблица 7.8

Требования к ресурсам и ПО сервера управления сетью хранения данных

Показатель	*Значение*
Центральный процессор	4 ядра
Оперативная память	Не менее 8 ГБ
НЖМД	Не менее 160 ГБ
Количество интерфейсов Ethernet	Не менее 2 ед., для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 ед, для отказоустойчивости

Показатель	*Значение*
Операционная система	MS Windows Server 2008 EE SP2 x64
База данных	Sybase
Средства отказоустойчивости	VMware HA

Таблица 7.9

Требования к ресурсам и ПО первого сервера управления ресурсами хранения

Показатель	*Значение*
Центральный процессор	8 ядер
Оперативная память	Не менее 24 ГБ
НЖМД	Не менее 160 ГБ
Количество интерфейсов Ethernet	Не менее 2 ед., для отказоустойчивости
Количество интерфейсов Fiber Channel	Не менее 2 ед., для отказоустойчивости
Операционная система	MS Windows Server 2008 EE SP2 x64
База данных	RDBMS
Средства отказоустойчивости	VMware HA

7.7. Общие решения по хранению сервисных данных и резервному копированию

Данные, которые использует подсистема мониторинга и управления, хранятся как локально в операционных системах, в которых запущены соответствующие приложения, так и в СУБД. Локальные данные хранятся на внешнем дисковом массиве и включены в существующие политики резервного копирования. Данные, хранящиеся в СУБД, защищаются средствами СУБД.

Технология виртуализации (например, VMWare) и технологии хранения (например, EMC) позволяют выделять на дисковом массиве ровно столько места, сколько реально используют серверы и виртуальные машины. Таким образом, объём презентованного места на хранилище с точки зрения хранилища будет меньше, чем с точки зрения виртуальных машин.

Резервное копирование данных серверов и баз данных производится согласно принятой технологии. Базы данных резервируются в режиме online.

7.8. Рекомендации по подготовке эксплуатационного персонала

В таблицах 7.10 – 7.12 представлен примерный состав курсов для подготовки квалифицированного персонала обслуживающего комплекс технических и программных средств.

Таблица 7.10

Список курсов по вычислительной платформе IBM

Название курса	*Примерная продолжительность (день)*
Введение в z/OS[10]	2
Основы работы в системе z/OS	4
Управление системой z/OS	3
Основы управления памятью	3
SMP/E для z/OS	4
OS/390 HCD и конфигурация аппаратных средств	4
Эффективное администрирование RACF	5

Таблица 7.11

Список курсов по администрированию СУБД на платформе IBM

Название курса	*Примерная продолжительность (день)*
Основы DB2	2
Подготовка по SQL	2
Администрирование баз данных DB2 для z/OS	5
Системное администрирование DB2 для z/OS	5
Восстановление данных в приложении DB2 для z/OS	3

[10] *z/OS — 64-битная серверная операционная система, разработанная компанией IBM для мейнфреймов.*

Рекомендации для специалистов по обслуживанию КТС в части подсистемы мониторинга

Таблица 7.12

Список курсов по подсистеме мониторинга и управления

Название курса	*Примерная продолжительность (день)*
IBM Tivoli Monitoring 6.2 для операторов и администраторов	4
Основы HP Systems Insight Manager (Windows/Linux) HP Systems Insight Manager 5.2, Rev. 8.43	4
EMC Ionix Service Assurance Manager Administrator	3

7.9. Рекомендации по технологическим помещениям и электроснабжению

Помещение хранилища данных соответствует строительным нормам СН-512-78 (Проектирование зданий и помещений для электронно-вычислительных машин) и удовлетворяет следующим требованиям:

- имеют ограниченный доступ (дверь и окна должны запираться);
- имеют достаточную площадь для размещения оборудования;
- имеют автоматические установки объемного газового пожаротушения;
- имеют вентиляцию и средства кондиционирования воздуха для поддержания климатических условий, необходимых для нормальной работы оборудования;
- имеют вводы силовой электросети и системы бесперебойного питания;

- имеют отдельную шину заземления (с сопротивлением не более 4 Ом);
- имеют освещение, соответствующее действующим санитарным нормам для технологических помещений.

Рабочие места обслуживающего персонала располагаются в других помещениях.

Качество электроэнергии соответствует показателям, установленным ГОСТ 13109-97 для промышленных сетей общего назначения и строительным нормам СН-512-78 для зданий и помещений для электронно-вычислительных машин:

- отклонение напряжения – не более 5%;
- коэффициент несинусоидальности – не более 5%;
- отклонение частоты – не более 0,2 Гц.

Кроме того, для обеспечения работы активного оборудования выполняются специальные требования, устанавливаемые ГОСТ 20397-82, ГОСТ 16325-88, ГОСТ 21552-84:

- высокочастотные напряжения в диапазоне частот 0,1–10 МГц не превышают по амплитуде 2% номинального напряжения сети;
- допускаются провалы напряжения глубиной 50% от номинального в течение одного периода и полное отключение в течение полупериода промышленной частоты, которые происходят не чаще 1 раза в секунду;
- импульсные напряжения могут быть с амплитудой не более 200% от амплитудного номинального напряжения длительностью 1 мс.

Заземление оборудования должно производится в соответствии с требованиями ГОСТ Р 50571.21-2000 «Заземляющие устройства и системы уравнивания электрических потенциалов в электроустановках, содержащих оборудование обработки информации».

Подключение к защитному заземляющему устройству должно выполняется кратчайшим путем, при помощи заземляющих проводов.

Каждое устройство подключается одним заземляющим проводом в установленном порядке. Приводятся в соответствие защитные заземления и зануления требованиям ГОСТ 12.1.030-81. Оборудование обязательно заземляется на контур заземления с сопротивлением не более 4 Ом.

В серверном помещении, предназначенном для размещения оборудования площадки, планируется модернизировать системы вентиляции и кондиционирования воздуха. Системы кондиционирования и вентиляции обеспечивают отвод тепла от оборудования.

Температурный и влажностный режим должен быть приведен в соответствие с требованиями (таблица 7.13), предъявляемыми оборудованием и согласно «Инструкции по проектированию зданий и помещений для электронно-вычислительных машин» (СН 512-78).

Таблица 7.13

Требуемые параметры температурно-влажностного режима

Оптимальные			*Допустимые*		
Температура воздуха, °С	*Относительная влажность воздуха, %*	*Скорость движения воздуха, м/с*	*Температура воздух, °С*	*Относительная влажность воздуха, %*	*Скорость движения воздуха, м/с*
21±2	47±7	Не более 0,2	18-26	Не более 75%	Не более 0,3

Рекомендуемые термины

Автоматизированное рабочее место – программно-технический комплекс АСУ, предназначенный для автоматизации деятельности определенного вида.

Виртуальная подсеть – логическое объединение ресурсов сети (АРМ, серверы, и т.п.) вне зависимости от их физического расположения. Взаимодействие ресурсов в пределах одной виртуальной сети осуществляется на канальном уровне (коммутация). Взаимодействие между виртуальными сетями осуществляется на сетевом уровне (маршрутизация).

Инстанция – отдельная инсталляция сервера приложений.

Объект информатизации (автоматизации) – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены.

Прикладное программное обеспечение – совокупность программ, предназначенных для решения задач, связанных с производственным процессом.

Система постоянной эксплуатации – сервер с установленным на нем программным обеспечением, предназначенным для постоянной эксплуатации.

Системный ландшафт – логическая структура элементов системы и схема переноса запросов на изменение между ними.

Система разработки – сервер с установленным на нем программным обеспечением, предназначенным для разработки, настройки и предварительного тестирования выполненных разработок и настроек.

Сетевое оборудование (сетеобразующее оборудование) – оборудование, использующееся для построения ЛВС и для организации взаимодействия различных ЛВС (концентраторы, коммутаторы, маршрутизаторы, серверы удаленного доступа).

Сеть хранения данных (англ. Storage Area Network, SAN) – архитектурное решение для подключения внешних устройств хранения данных, таких как дисковые массивы, ленточные библиотеки, оптические приводы к серверам таким образом, чтобы операционная система распознала подключённые ресурсы как локальные.

Семейство ОС Windows – операционные системы корпорации Microsoft: Windows 95, Windows 98, Windows Me, Windows NT Server и Workstation, Windows 2000 Server и Professional, Windows XP Professional, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008. В зависимости от контекста использования «АРМ» или «сервер» может опускаться часть полного названия ОС: сервер под управлением ОС Windows 2000 (пропущено «Server»). При необходимости указать несколько операционных систем используется обозначения вида «Windows95/98/NT/2000». Если нет необходимости выделения типа ОС (серверная или клиентская), то соответствующее название также сокращается.

Системный администратор – лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Системно-техническая платформа – совокупность программных и технических элементов систем обработки, хранения, обмена и ввода/вывода

данных, способных функционировать самостоятельно или в составе других систем.

Тестовая система – сервер с установленным на нем программным обеспечением, предназначенным для окончательного тестирования и проверки совместимости с рабочей версией, а также для обучения конечных пользователей.

Рекомендуемые сокращения

DLNA (англ. Digital Living Network Alliance) – стандарт, позволяющий совместимым устройствам передавать и принимать по сети различный медиа-контент (изображения, музыку, видео), а также отображать его в режиме реального времени.

DMS (Document management system) – система программного обеспечения для отслеживания и хранения электронных документов и/или цифровых образов документов.

NAS (англ. Network Attached Storage) – сетевая система хранения данных, сетевое хранилище.

АПК – аппаратно-программный комплекс

АРМ – автоматизированное рабочее место

АСБУ – автоматизированная система бюджетного управления

АСКО – автоматизированная система формирования консолидированной отчетности

АСУ ТОиР – автоматизированная система управления техническим обслуживанием и ремонтом

БД – база данных

ВИР – вертикально-интегрированные решения

ВК – вычислительный комплекс

ВМ – виртуальная машина

ЕВСПД – единая ведомственная сеть передачи

ИВС – информационно-вычислительная система

ИУС – информационно-управляющая система

КТС – комплекс технических средств

КХД – корпоративное хранилище данных

ЛВС – локальная вычислительная сеть

ММУ – модуль мониторинга и управления

МЭДО – межведомственный электроны документооборот

ОЗУ – оперативное запоминающее устройство

ОС – операционная система

ПО – программное обеспечение

ПОИБ – подсистема обеспечения информационной безопасности

СДКХ – служба доступа к корпоративному хранилищу данных

СДП – служба доступа пользователей

СКП – служба каталога пользователя

СМЭВ – система межведомственного электронного документооборота

ССРП – служба совместной работы пользователей

СТИ – системно-техническая инфраструктура

СУБД – система управления базами данных

СФД – служба файлового доступа

СХД – система хранения данных

СЭД, СЭДО – система электронного документооборота

УЦ – управляющий центр

ФОИВ – федеральный орган исполнительной власти

ЦОД – центр обработки данных

ЦП – центральный процессор

ЦХЭД – центр хранения электронной документации

ЭДО – электронный документооборот

ЭФП – электронный фонд пользования

Выводы

1. Вопросы передачи электронных документов из СЭД ФОИВ в центр хранения электронных документов требуют создания нормативно-правовой базы.

2. При организации взаимодействия между СЭД ФОИВ и хранилищем электронных документов ЦХЭД необходимо использовать защищенный канал подключения к сети Интернет.[11]

3. Безопасность хранения данных в хранилище ЦХЭД должна определяться требованиями национального стандарта Российской Федерации ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения» и требованиям по технической защите конфиденциальной информации.

4. Система хранения электронных документов в хранилище ЦХЭД должна использовать сертифицированные в соответствии с требованиями безопасности информации технические и программные средства защиты информации.

5. Хранилище данных ЦХЭД должно обеспечивать управление документов, имеющих электронные цифровые подписи и соответствовать требованиям, установленным Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

6. Система хранения данных ЦХЭД должна обеспечивать работу с форматами электронных документов Portable Document Formatt (pdf), Rich Text Format (rtf), Document (doc), Tagged Image File Format (tiff).

Также допускать по необходимости работу с другими форматами файлов.

---

[11] Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» (Собрание законодательства Российской Федерации, 2008, № 12, ст. 1110; 2008, № 43, ст. 4919; 2011, № 4, ст. 572).

7. Система хранения данных ЦХЭД должна иметь характеристики обработки информации, которые не приводили бы к ухудшению характеристик функционирования СЭД ФОИВ при взаимодействии СЭД ФОИВ и системой государственного хранения электронных документов.

8. Системно-техническая инфраструктура хранения электронных документов создается в соответствии с разработанными рекомендациями.

Список источников

1. *Буйлов О.* Сравнение «облачных» хранилищ данных. // URL: http://softkey.info/reviews/review12389.php
2. Официальная страница «облачного» хранилища данных SkyDrive: https://login.live.com/login.srf
3. Официальная страница «облачного» хранилища данных DropBox: https://www.dropbox.com
4. Официальная страница «облачного» хранилища данных GoogleDrive: https://www.google.com/intl/ru/drive/start/index.html
5. Официальная страница «облачного» хранилища данных Яндекс.Диск: http://disk.yandex.ru/
6. Электронный ресурс LiveBusiness: http://www.livebusiness.ru/tags/oblachnye_platformy/
7. Ежемесячный информационный журнал Neue Zeiten: http://neuezeiten.rusverlag.de/2012/08/27/1536-3/
8. Официальная страница проекта Национальной облачной платформы О7: http://www.rostelecom.ru/projects/innovations/o7/

Приложение 1

МИНИСТЕРСТВО СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

02.09.2011 №221

Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения

В соответствии с пунктом 5.2.23 Положения о Министерстве связи и массовых коммуникаций Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 2 июня 2008 г. № 418 (Собрание законодательства Российской Федерации, 2008, № 23, ст. 2708; № 42, ст. 4825; № 46, ст. 5337; 2009, № 3, ст. 378; № 6, ст. 738; № 33, ст. 4088; 2010, № 13, ст. 1502; № 26, ст. 3350; № 30, ст. 4099; № 31, ст. 4251; 2011, № 2, ст. 338; № 3, ст. 542; № 6, ст. 888; № 14, ст. 1935; № 21, ст. 2965), и пунктом 2 плана мероприятий по переходу федеральных органов исполнительной власти на безбумажный документооборот при организации внутренней деятельности, утвержденного распоряжением Правительства Российской Федерации от 12 февраля 2011 г. № 176-р (Собрание законодательства Российской Федерации, 2011, № 8, ст. 1151),

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые требования к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающие в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения (далее – Требования).

2. Департаменту государственной политики в области создания и развития электронного правительства (Липов) опубликовать Требования на официальном сайте Министерства связи и массовых коммуникаций Российской Федерации в информационно-телекоммуникационной сети Интернет.

3. Направить настоящий приказ на государственную регистрацию в Министерство юстиции Российской Федерации.

Министр И.О. Щёголев

Приложение 2

Анкета
Характеристика хранения электронных документов в СЭД ФОИВ

1. Наименование Федерального органа исполнительной власти:

2. Есть ли внутриведомственные нормативные документы регламентирующие работу СЭД?

ДА НЕТ (нужное подчеркнуть)

3. Форматы электронных документов применяемые в СЭД:

4. Возможные форматы выгрузки электронных документов из СЭД:

5. Хранение электронных документов в СЭД:

- CD/DVD отдельные диски
- CD/DVD библиотеки
- серверное хранение
- система хранения на жестких дисках
- ленточная библиотека
- другое (указать какое)

6. Есть ли резервное копирование на магнитную ленту?

ДА НЕТ (нужное подчеркнуть)

7. Возможная передача электронных документов из СЭД на государственное хранение на носителях:

- магнитная лента
- CD/DVD диски
- сеть Интернет

8. Наличие в электронных документах СЭД электронно-цифровой подписи (ЭЦП):

ДА НЕТ (нужное подчеркнуть)

9. Текущий объем хранения электронных документов в СЭД (на « _____ 20_____г.»):

Мбайт

10. Ежегодный прирост объема хранения (примерный, ожидаемый):

Мбайт

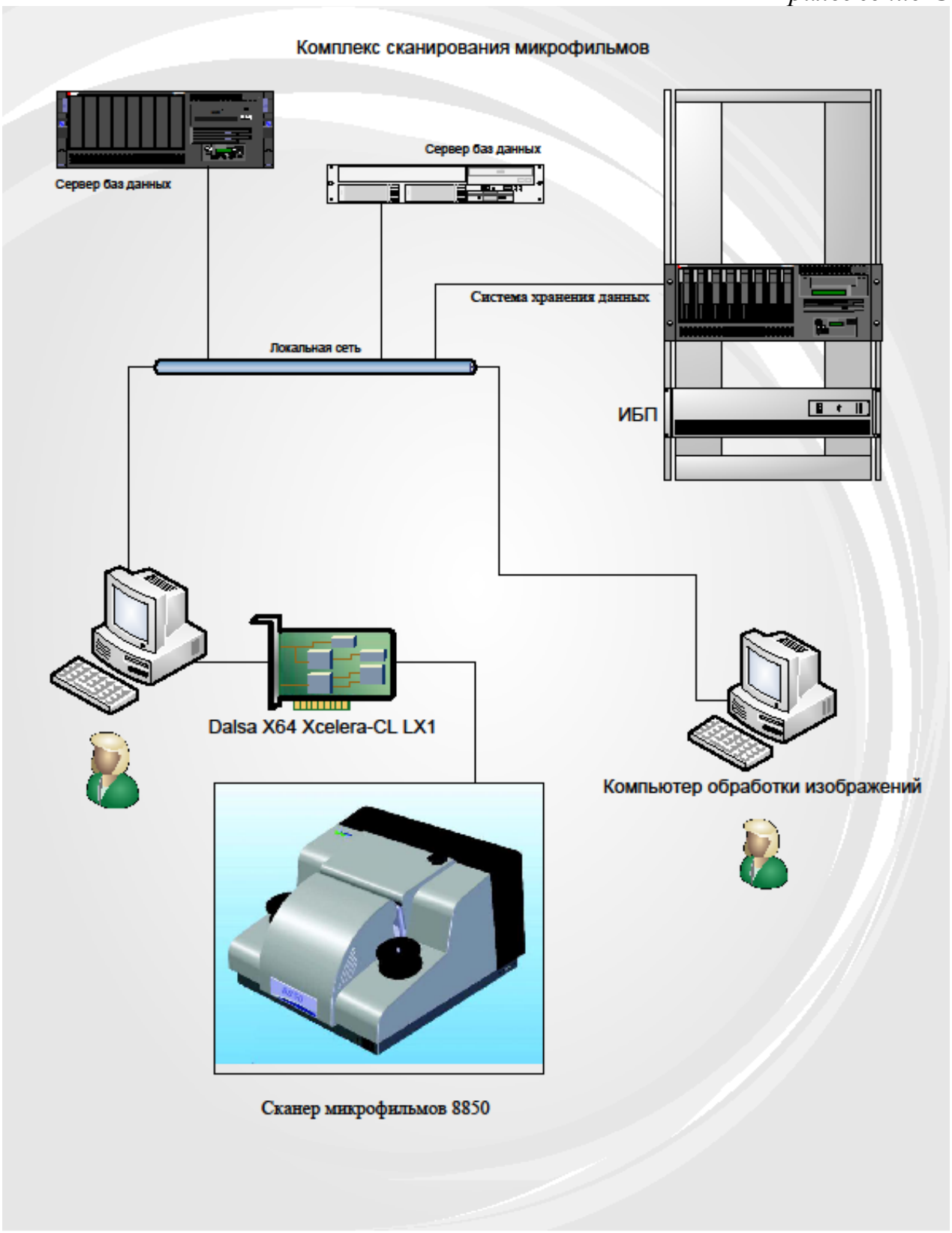
_____

подпись ФИО уполномоченного лица

Контактный телефон уполномоченного лица:

Адрес электронной почты уполномоченного лица:

Приложение 3



Приложение 4

Соответствие компьютерного оборудования и программного обеспечения требованиям безопасности

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Оборудование и ПО должны иметь функции* контроля доступа, идентификации (аутентификации), контроля целостности, аудита и мониторинга, криптографии (при необходимости), а так же быть интегрирована с инфраструктурой открытых ключей в целях обеспечения разграничения доступа к обрабатываемой в них информации на уровне отдельных программных модулей и структур данных.

Оборудование и ПО должны обеспечивать выполнение требований законодательства по защите персональных данных в соответствии с Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

Конструкция используемого оборудования должна обеспечивать безопасность эксплуатирующего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007.

Должны быть обеспечены безопасность при монтаже, наладке, эксплуатации, обслуживании и ремонте оборудования, включая защиту от воздействий электрического тока, электромагнитных полей, акустических шумов, а также требования по допустимым уровням освещенности, вибрационных и шумовых нагрузок, при необходимости.

Приложение 5

Нормативно-технические документы

Федеральный закон от 17 июля 1999 года N 181-ФЗ "Об основах охраны труда в Российской Федерации".

Федеральный закон Российской Федерации от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании".

Федеральный закон Российской Федерации от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации".

Федеральный закон Российской Федерации от 8 июля 2006 г. N 152-ФЗ "Закон о персональных данных".

ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.

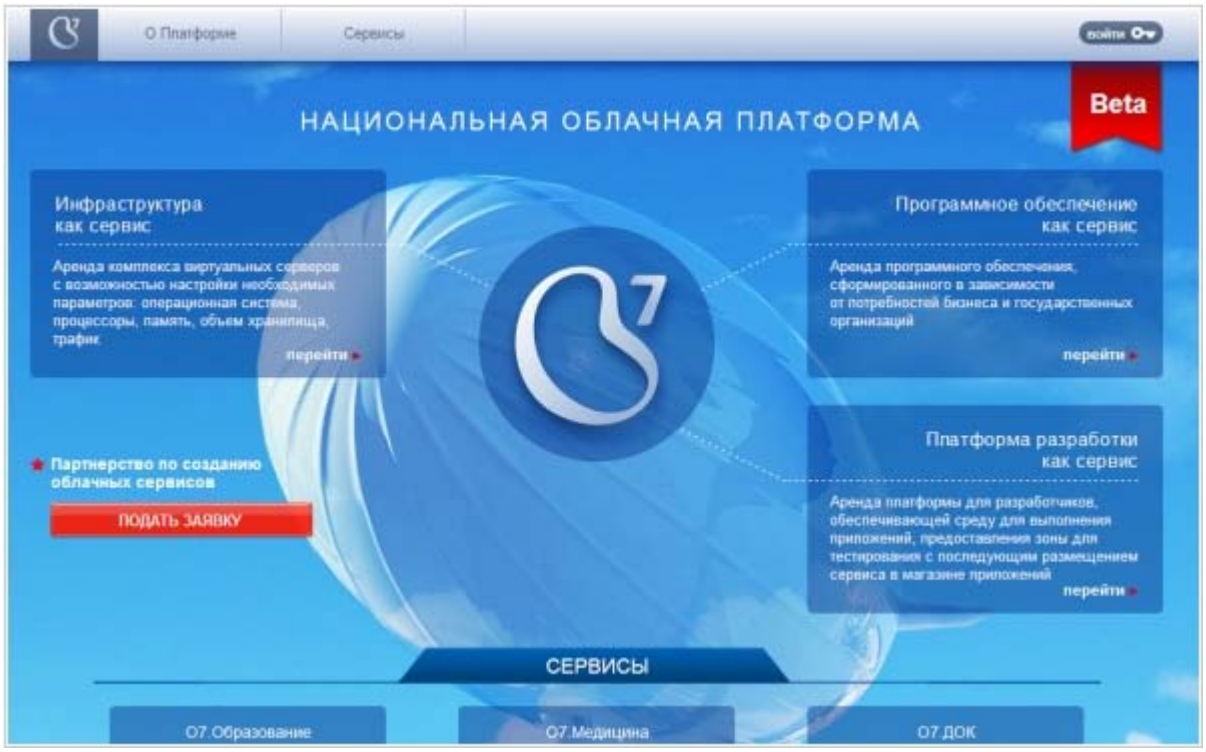
Рекомендации о порядке учета, оперативного хранения и отбора на постоянное хранение электронных документов. М.2005. ВНИИДАД

Методические рекомендации по организации хранения, комплектования, учета и использования электронных документов в государственных архивах. Москва, ВНИИДАД, 2007.

Рекомендации по созданию оцифрованных копий фонда пользования фото и фонодокументов. Москва, РГАНТД, 2008.

Приложение 6

Проект Национальная облачная платформа



Работа по созданию Национальной облачной платформы О7 началась в марте 2011 года, и уже через год она была запущена в опытную эксплуатацию.

Национальная облачная платформа – это комплекс интегрированных информационных систем, предназначенный для предоставления органам исполнительной власти различного уровня, органам местного самоуправления, коммерческим организациям и физическим лицам услуг по модели облачных вычислений.

Успешно запущены и работают в тестовом режиме онлайн-сервисы: О7. Медицина, О7. Образование, О7. ЖКХ, О7. Сити, О7. 112, а также сервисы для малого и среднего бизнеса: О7. ДОК и О7. Бизнес.

Для продвижения национальной облачной платформы «Ростелеком» создал портал О7.com, через который можно связаться с менеджерами Инновационного центра. Пользователи могут получить через Портал оперативную информацию о продуктах, предлагаемых компанией

«Ростелеком» и её партнерами, а разработчики – пройти экспертизу своих решений или предложить разработку. Видя гигантский экспортный потенциал в тех сервисах, которые «Ростелеком» может предложить уже сегодня, компания сразу выбрала для платформы доменное имя в международной зоне «com».

Основные преимущества использования облачных технологий в модели SaaS (программное обеспечение как услуга):

- отсутствие затрат на приобретение, установку, обновление и поддержание
- работоспособности дорогостоящего оборудования, а также работающего
- на нём программного обеспечения
- сокращение затрат на внедрение новых систем в 30 раз
- 5-кратное сокращение сроков внедрения новых систем
- обеспечение безопасности информации в соответствии с действующими нормами

Описание сервисов Национальной облачной платформы О7
на сайте ОАО «Ростелеком»:
http://www.rostelecom.ru/projects/innovations/o7/BOOKLET_12_06.7z