

УТВЕРЖДАЮ

Курбанов М. М.
Председатель Узкомгосрезерв
21 июня 2021 года

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание автоматизированной системы электронного документооборота
Комитета по управлению государственными резервами при Кабинете
Министров Республики Узбекистан (Узкомгосрезерв)

на 45 листах

действует с 21.06.2021г.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ	7
1.1. Полное наименование ИС и ее условное обозначение.....	7
1.2. Наименование организаций заказчика и разработчика ИС.....	7
1.3. Перечень документов, на основании которых создается ИС.....	7
1.4. Плановые сроки начала и окончания работ	7
1.5. Порядок оформления и предъявления результатов работ.....	7
1.6. Внесение изменений и дополнений к ТЗ	7
2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИС	7
2.1. Назначение ИС	7
2.2. Цели создания ИС	8
3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ	8
3.1. Краткие сведения об объекте информатизации	8
3.2. Сведения об условиях эксплуатации объекта информатизации и характеристиках окружающей среды	10
4. ТРЕБОВАНИЯ К ИС	10
4.1. Требования к ИС в целом	10
4.1.1. Требования к структуре и функционированию ИС.....	11
4.1.1.1. Перечень подсистем, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации ИС	11
4.1.1.2. Перечень сторонних ИС с которыми должно обеспечено взаимодействие	13
4.1.1.3. Требования к режимам функционирования ИС	13
4.1.1.4. Перечень и описание сценариев использования ИС	14
4.1.1.5. Требования по диагностированию ИС	23
4.1.1.6. Перспективы развития, модернизации ИС	23
4.1.2. Требования к взаимодействию со сторонними информационными системами	23
4.1.2.1. Общие требования к взаимодействию.....	23
4.1.2.2. Представление исходящего электронного документа в виде XML-документа для передачи между различными СЭД.....	24
4.1.3. Требования к численности и квалификации персонала ИС и режиму его работы	24
4.1.3.1. Требования к численности персонала (пользователей) ИС	24
4.1.3.2. Требования к квалификации персонала, порядку его подготовки и контроля знаний и навыков.	24
4.1.3.3. Требуемый режим работы персонала ИС.....	25
4.1.4. Показатели назначения.....	25
4.1.4.1. Значения параметров, характеризующие степень соответствия ИС по назначению	25

4.1.4.2.	Вероятностно-временные характеристики, при которых сохраняется целевое назначение ИС	25
4.1.5.	Требования к надежности	26
4.1.5.1.	Состав и количественные значения показателей надежности для ИС в целом или её подсистем	26
4.1.5.2.	Перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей	26
4.1.5.3.	Требования к надежности технических средств и программного обеспечения	27
4.1.5.4.	Требования к методам оценки и контроля показателей надежности на разных стадиях создания ИС	28
4.1.6.	Требования к безопасности	28
4.1.6.1.	Требования безопасности технических средств	28
4.1.6.2.	Требования к защите информации от несанкционированного доступа	28
4.1.6.3.	Требования к обеспечению информационной безопасности системы с применением электронно-цифровой подписи	30
4.1.6.4.	Требования по сохранности информации при авариях	31
4.1.6.4	Требования к защите от влияния внешнего воздействия	31
4.1.7.	Требования к эргономике и технической эстетике	31
4.1.8.	Требования к патентной и лицензионной чистоте	32
4.1.9.	Требования по стандартизации и унификации	32
4.2.	Требования к функциям (задачам), выполняемым ИС	32
4.2.1.	Общие требования к делопроизводственным функциям	33
4.2.2.	Требования к функциям контроля исполнения	36
4.2.3.	Требования к поддержке процессов подготовки и согласования документов	36
4.2.4.	Требования к возможностям настройки Системы	36
4.2.5.	Требования к электронному документу в Системе	37
4.2.6.	Требования к справочникам Системы	37
4.2.7.	Требования к схеме классификации, форматам и типам документов в Системе	37
4.3.	Требования к видам обеспечения	38
4.3.1.	Требования к математическому обеспечению	38
4.3.2.	Требования к информационному обеспечению	38
4.3.3.	Требования к лингвистическому обеспечению	39
4.3.4.	Требования к программному обеспечению	39
4.3.5.	Требования к техническому обеспечению	40
4.3.6.	Требования к организационному обеспечению	40
4.3.7.	Требования к методическому обеспечению	41

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС.	43
6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС.	43
6.1. Виды, состав, объем и методы испытаний системы и ее составных частей.	44
6.1.1. Предварительные испытания.	44
6.1.2. Опытная эксплуатация.	44
7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ИС К ВВОДУ В ДЕЙСТВИЕ.	45
8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ.	45

Термины и определения

Метаданные	Набор структурированных данных, включающих реквизиты, которые наследуются вследствие определенного положения папки в схеме классификации
Сервер	Компьютер (или специальное компьютерное оборудование), выделенный и специализированный для выполнения определенных сервисных функций
Системный журнал	Документ, в который записываются действия пользователей или администратора, а также действия, выполнение которых инициировано СЭД вследствие заданных системных параметров
Рабочая станция	Компьютер в составе локальной вычислительной сети по отношению к серверу
Регистрационно-учетная карточка	Карточка, предназначенная для регистрации электронного документа в делопроизводстве организации

Сокращения

Сокращение	Полная форма/определение
АСОД	Автоматизированная система обработки данных
БД	База данных
ДСП	Для служебного пользования
ИС	Информационная система
ИБ	Информационная безопасность
ИБП	Источник бесперебойного питания
КП	Контрольный пункт
КТС	Комплекс технических средств
ЛВС	Локальная вычислительная сеть
ОС	Операционная система
РС	Рабочая станция
ПК	Персональный компьютер
ПО	Программное обеспечение
СЗИ	Средства защиты информации
СКЗИ	Средства криптографической защиты информации
СУБД	Система управления базами данных
СЭД	Система электронного документооборота
ТСИ	Технические средства информатизации
ЭВМ	Электронно-вычислительная машина
ЭЦП	Электронная цифровая подпись
TCP/IP	Transmission Control Protocol/Internet Protocol(Протокол Контроля Передачи/Протокол Интернета)
VPN	(Virtual Private Network) - виртуальная частная сеть
XML	(Extensible Markup Language) - расширяемый язык разметки

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование ИС и ее условное обозначение

Полное наименование ИС: Автоматизированная система электронного документооборота Комитета по управлению государственными резервами при Кабинете Министров Республики Узбекистан (Узкомгосрезерв).

Условное обозначение: СЭД, ИС, Система.

1.2. Наименование организаций заказчика и разработчика ИС

Заказчиком ИС является Комитет по управлению государственными резервами при Кабинете Министров Республики Узбекистан (Узкомгосрезерв).

Адрес: 100084, г.Ташкент, ул. Халкобод, д. 17а

E-mail: info@udz.uz

Исполнитель ИС будет определен по итогам конкурсных (тендерных) торгов.

1.3. Перечень документов, на основании которых создается ИС

Основанием для разработки является []

Перечень документов, на основании которых должна разрабатываться ИС приведена в п.4.3.9. Требования к методическому обеспечению.

1.4. Плановые сроки начала и окончания работ

ИС должна быть реализована в течении 3 месяцев с даты заключения договора на разработку программного обеспечения.

1.5. Порядок оформления и предъявления результатов работ

Оформление и предъявление результатов работ по созданию ИС осуществляются согласно разделу 6 настоящего ТЗ.

1.6. Внесение изменений и дополнений к ТЗ

Настоящее Техническое задание может дополняться или изменяться в процессе внедрения и технического сопровождения ИС. Изменения к ТЗ должны содержать основание для изменения, содержания изменения и ссылки на документы, в соответствии с которыми вносятся эти изменения. Все изменения оформляются в порядке, установленном для ТЗ (титульный лист изменения к ТЗ оформляют аналогично титульному листу ТЗ и пишут «Изменение №... к ТЗ на ИС...»). Изменения к ТЗ являются неотъемлемой частью ТЗ на ИС. Изменения к ТЗ на ИС не допускается утверждать после представления ИС на приемо-сдаточные испытания.

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ ИС

2.1. Назначение ИС

Система предназначена для автоматизации работ с распорядительными, подготовленными и поступившими документами, их обработки, хранения, регистрации, уничтожения и формирования отчетов, а также ведения электронного архива документов в Узкомгосрезерв, а также их структурных, территориальных и подведомственных подразделениях.

Система направлена:

- на совершенствование планирования, контроля выполняемых мероприятий;
- на совершенствование системы делопроизводства с применением новых средств и методов управления;
- на интеграцию с другими системами обработки данных;
- для взаимосвязи с другими СЭД;
- для автоматизации информационного обеспечения сотрудников;
- на создание единой системы учета документов в электронном виде;
- для систематизации регистрации документов;

- для контроля исполнения документов;
- для обеспечения конфиденциальности, целостности и доступности информации в электронном виде.

2.2. Цели создания ИС

Целями создания Системы являются:

- создание электронного документооборота во всех подразделениях Узкомгосрезерв, а также формирование электронных файлов для передачи в другие СЭД министерств и ведомств республики;
- сокращение времени прохождения и поиска документов по подразделениям Узкомгосрезерв;
- экономия ресурсов за счет сокращения издержек по управлению потоками бумажных документов в подразделениях Узкомгосрезерв;
- распределение задач плана мероприятий между ответственными сотрудниками;
- ведение контроля выполнения плановых мероприятий;
- формирование базы распорядительных документов;
- систематизация и унификация технологии работы с документами;
- создание системы учета и хранения документов в электронном виде, их систематизация и контроль исполнения;
- унификация процессов делопроизводства и документооборота для взаимодействия с Системой;
- соблюдение принципа однократности регистрации документов;
- повышение эффективности и оперативности работы с документами;
- организация управленческого документооборота в электронном виде;
- автоматизация процессов принятия решений;
- усиление контроля исполнительской дисциплины;
- определение состава форм представления оперативных отчетов и форм для проведения статистического анализа исполнения поручений;
- обеспечение сбора и анализа данных о ходе исполнения документов, плановых мероприятий в режиме реального времени;
- повышение качества информационного обеспечения сотрудников;
- исключение утери документов и сокращение числа ошибок при обработке больших потоков документов;
- формирование отчетов по выполненным мероприятиям согласно плану мероприятий из предоставленных сведений сотрудников;
- обобщение отчетов выполнения плановых мероприятий подразделения;
- обеспечение высоких требований защиты информации на всех этапах жизненного цикла электронных документов в Системе;
- улучшение качества, полноты и достоверности информации с соблюдением условий ИБ;
- обеспечение аутентификации пользователей и распределение уровня доступа при их доступе к системам, средствам и информационным ресурсам;
- обеспечение сохранности данных в процессе хранения, передачи и обработки, в соответствии с требованиями ИБ.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

3.1. Краткие сведения об объекте информатизации

Пользователями информационного взаимодействия в Системе являются сотрудники Узкомгосрезерв и его подразделений. Мониторинг состояния и контроль исполнительской дисциплины на местах осуществляют руководители подразделений Узкомгосрезерв или ответственные за контроль лица.

Объектами автоматизации являются процессы подготовки, обработки, регистрации, рассмотрения, ознакомления, хранения документов, а также планирования и отчетности,

осуществления мониторинга, оперативного контроля исполнительской дисциплины, информационного взаимодействия подразделений Узкомгосрезерв.

Автоматизации подлежат процессы:

- формирования плана мероприятий Узкомгосрезерв;
- распределения задач плановых мероприятий между ответственными сотрудниками подразделений Узкомгосрезерв;
- рассылки документов и поручений;
- регистрации, ознакомления и хранения распорядительных документов;
- рассмотрения и согласования документов;
- поиска документов;
- сбора данных о ходе исполнения документов и поручений;
- формирования отчетов и аналитических справок по собранным данным;
- формирования бланков электронных документов;
- формирования базы данных распорядительных документов;
- формирования листа согласования;
- формирования дел и журналов.

Система должна обеспечивать доступ к собственным ресурсам в режиме 24/7/365.

Сведения об условиях расположения оборудования

Оборудование, предназначенное для функционирования Системы, устанавливается в помещениях Узкомгосрезерв, отвечающих требованиям стандарта O'z DSt 2875:2014.

Установка серверного оборудования системы предусматривается в существующих серверных помещениях с действующими системами вентиляции и кондиционирования, системой бесперебойного энергоснабжения в составе дизель-генераторной установки и системой технологического заземления. Минимальные требования в соответствии с O'z DSt 2875-2014 к климатическим условиям в существующих помещениях. Требования стандартов к размещению оборудования: O'z DSt 2875-2014 - Информационная технология. Требования к дата-центрам. Инфраструктура и обеспечение информационной безопасности; RH 45-169:2004 - Основные требования к организации межведомственной компьютерной сети; RH 45-201:2011 - Технические требования к зданиям и сооружениям для установки средств вычислительной техники в существующих помещениях.

Критически важные сегменты Системы должны быть дублированы и установлены в помещениях (зданиях) максимально удаленных от основных помещений (зданий) Узкомгосрезерв.

Телекоммуникационное оборудование и оборудование взаимосвязи (телекоммуникационное оборудование, обеспечивающее взаимосвязь серверного оборудования и межсетевых экранов) будут установлены по отдельности.

Пользовательские терминалы могут находиться в удаленных зданиях Узкомгосрезерв.

Условия эксплуатации объекта автоматизации и характеристики окружающей среды применительно к персоналу должны соответствовать требованиям, предъявляемым санитарными правилами и нормами, обеспечиваемыми Заказчиком.

Условия эксплуатации объекта автоматизации и характеристики окружающей среды применительно к техническим средствам должны соответствовать требованиям, приведенным в технической документации на эти средства.

На объектах автоматизации должны отсутствовать такие воздействия, как: механический резонанс, синусоидальная вибрация, механические удары, атмосферное пониженное давление, плесневые грибы, рабочие растворы и агрессивные среды.

Электропитание на стационарных объектах эксплуатации осуществляется от электрической сети напряжением 380/220В, частотой 50 Гц с глухо заземленной или изолированной нейтралью и обеспечивается резервирование.

3.2. Сведения об условиях эксплуатации объекта информатизации и характеристиках окружающей среды

Пользователи выполняют свои обязанности в закрытых помещениях, не подверженных вредным воздействиям и удовлетворяющих требованиям по установке средств вычислительной техники. Характеристики окружающей среды в помещениях объектов информатизации применительно к персоналу определяются в соответствии с нормами охраны труда и техники безопасности, установленными в Республике Узбекистан и «Санитарными правилами и нормами при работе на персональных компьютерах, видео-дисплейных терминалах и оргтехнике» (СанПиН № 0224-07 от 03.04.07).

4. ТРЕБОВАНИЯ К ИС

4.1. Требования к ИС в целом

ИС предназначена для автоматизации технологических и информационных процессов ведения документооборота и планирования мероприятий, а также контроля их выполнения в Узкомгосрезерв, включая их подразделения.

Система должна:

- обеспечивать совместную работу с защищенной сетью передачи данных «VECTOR» и с АСОД «НИМОУА»;
- обеспечивать картотечную регистрацию документов (подготовленных, входящих и распорядительных);
- обеспечивать формирование плана мероприятий и распределение задач;
- быть гибкой и адаптируемой к изменениям внешних условий (например, изменению законодательства или внутриведомственных актов), что обеспечивает снижение затрат на ее поддержку и сопровождение;
- функционировать в web-ориентированной архитектуре;
- допускать эволюционный характер создания и последующего развития путем постепенного наращивания функций;
- создаваться по модульному принципу, позволяющему легко расширять функциональность Системы;
- выдвигать минимальные требования к аппаратно-техническим средствам и квалификации обслуживаемого персонала;
- использовать ЭЦП для подписания электронных документов;
- использовать сертифицированные СКЗИ для хранения и передачи критических информационных ресурсов Узкомгосрезерв;
- иметь удобный для пользователя и администратора интерфейс;
- предоставлять возможность формирования отчетов действий системы, пользователей и администратора;
- предоставлять возможность формирования делопроизводственных отчетов.

Система должна выполнять следующие функции:

- формирование электронного сообщения, содержащего набор значений реквизитов документа, документа в электронном виде и другую необходимую информацию;
- прием и обработка поступившего в Систему электронного сообщения или документа, в соответствии с технологией, установленной данной Системой;
- анализ результата приема поступившего электронного сообщения, формирование и отправка уведомления (ответного электронного сообщения), содержащего информацию о доставке, прочтении электронного сообщения, об ошибках приема и интерпретации электронного сообщения, о регистрации полученного документа и т.п.;
- формирование отчетов по выполненным мероприятиям согласно плану мероприятий из электронных сообщений сотрудников;
- напоминание о днях рождений сотрудников;
- контроль присутствия сотрудников;
- организация хранения электронных документов, а также работы с ними (в частности, их поиска);
- передача документа-ответа, являющегося результатом исполнения документа.

Принципами построения и обеспечения функционирования Системы должны являться:

- использование технических и программных средств, соответствующих единым требованиям;
- обеспечение технологической возможности информационного взаимодействия Системы с программным обеспечением, устройствами ввода вывода, а также другими СЭД ведомств республики посредством XML документа;
- применение средств ЭЦП для обеспечения юридической значимости документа в Системе;
- применение сертифицированных СКЗИ в Системе;
- реализация единых технологических принципов форматов, протоколов и регламентов информационного взаимодействия;
- обеспечение требуемого уровня ИБ при информационном взаимодействии между подразделениями;
- наличие формализуемых процедур автоматизации контроля функций документооборота (подготовка документов определенного типа, отправка, уничтожение и т.п.);
- наличие развитых средств поиска информации;
- полная поддержка Системой различных языков, используемых в имеющихся документах Заказчика.

4.1.1. Требования к структуре и функционированию ИС

Архитектурно Система должна быть реализована в Web-ориентированном клиент-серверном варианте. В качестве инфраструктурного программного обеспечения (сервер приложений, сервер базы данных) должны использоваться бесплатное «open-source» или лицензированное программное обеспечение, обеспечивающие обработку 1000 одновременных запросов и 1 ГБ поточных данных.

Система должна включать в себя:

- централизованную базу данных Узкомгосрезерв, устанавливаемую на серверы с обеспечением программно-технических и организационных мер защиты информации во время хранения и использования соответствующих информационных ресурсов, обеспечивающую защищенное хранение всех электронных документов;
- централизованное хранилище критического информационного ресурса Узкомгосрезерв, обеспечивающее программно-технические, криптографические и организационные меры защиты информации во время хранения и использования;
- Web-сервер для функционирования компонентов Системы, реализованный в виде набора Web-приложений и служб;
- клиентскую программу, устанавливаемую на рабочих станциях пользователей, с элементами авторизации пользователей и рабочей станции в Системе на дискреционной и мандатной основах, а также обеспечивающее удаление всех временных файлов (из оперативной памяти, временных копий файлов из накопителей).

В состав СЭД должно также входить аппаратно-программное, аппаратное и программное СКЗИ, имеющее сертификат соответствия по требованиям информационной безопасности (или заключение Уполномоченного органа), используемое для формирования и проверки ЭЦП и криптографического шифрования информации.

4.1.1.1. Перечень подсистем, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации ИС

В состав программного обеспечения Системы должны входить следующие подсистемы и модули:

1. Подсистема управления доступом документооборота в составе:

- модуля маршрутизации документов, предназначенного для обеспечения пересылки документов на рабочие места исполнителей, сбора информации о текущем статусе документов, осуществления консолидации документов по завершении работы с ними на отдельных этапах, а также обеспечения пользователей средствами доступа к информации о текущем состоянии работ с документами;

- модуля авторизации и аутентификации пользователей Системы;
- модуля общего конфигурирования Системы, обеспечивающего настройки её параметров и технических характеристик;
- модуля ведения справочников и классификаторов, включающего:
 - наименование подразделений, физических и юридических лиц и соответствующие им электронные и физические адреса;
 - вид и тип электронного документа;
 - характер вопроса электронного документа;
 - наименование области, района, города, населенного пункта;
 - типовые маршруты движения электронных документов;
 - перечень должностей, должностных лиц и др.
- модуль мониторинга администратора системы;
- модуль мониторинга сетевой активности пользователей Системы и системного администратора;

2. Подсистема регистрации и учета в составе:

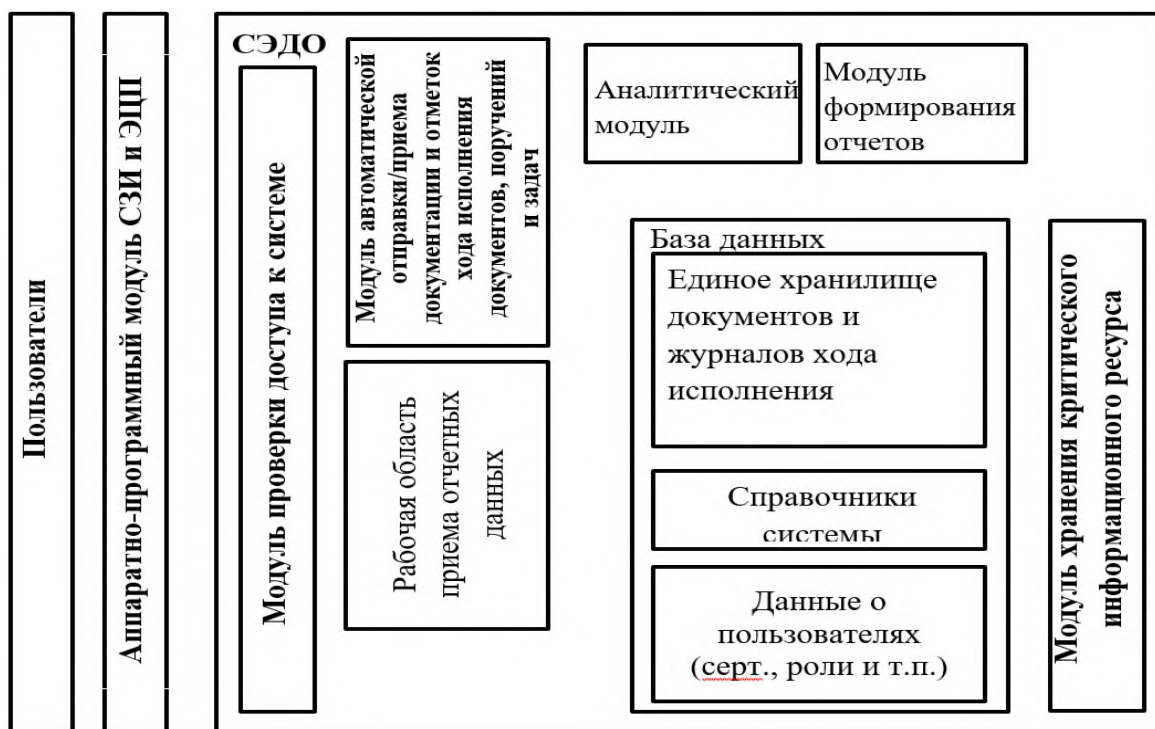
- модуля текущего ввода документов, предназначенного для обеспечения ввода новых, поступивших документов и распечатки электронных документов на бумажный носитель информации;
- модуля формирования плана мероприятий и распределения задач;
- модуля поиска документов, предназначенного для индексации и поиска учётных записей, дел и документов на основании реквизитов и их атрибутов;
- модуль хранения критического информационного ресурса, включающий в себя:
 - а) единое хранилище распределительных документов;
 - б) хранилища номенклатурных дел;
 - в) хранилища точек восстановления ПО и резервных копий БД;
 - г) хранилища системных журналов (лог, конфигурационные файлы, системные журналы ОС и СЭД).
- модуля формирование и обобщение отчетов по выполнению плановых мероприятий, включающего в себя:
 - а) модуль формирования отчетов по выполненным пунктам плана мероприятий;
 - б) модуль формирования отчетов по документам (контрольным, входящим, исходящим), контрольным пунктам, исполнительской дисциплине, статистические и т.п.
 - в) модуль формирования отчетов администратора по информационной безопасности;
 - г) модуль формирования отчетов администратора системы;
- модуля регистрации, ознакомления и хранения распорядительных документов;
- модуля формирования баз данных распорядительных документов;
- аналитический модуль, предназначенный для обработки информации о состоянии исполнительской дисциплины путем формирования запросов, аналитических материалов и генерации отчетных форм;

3. Подсистема обеспечения целостности и криптографии в составе:

- модуля верификации и атрибутирования документов, предназначенного для обеспечения возможности ввода информации о документе и редактирования пользователем электронной версии документа;
- модуля электронной цифровой подписи;
- модуля криптографической защиты информации, обеспечивающего шифрование информации в Системе;
- модуль резервирования БД, критического информационного ресурса и восстановления;
- модуль зеркалирования БД и критического информационного ресурса;
- модуля организации связи, предназначенного для обеспечения связи между подсистемами и модулями Системы, а также обмена данными внутри Системы.

4. Подсистема управления и диспетчеризации электронных документов в составе:

- модуль управления размещением и рассылкой документов, а также оповещение исполнителей;
- модуль мониторинга администратора системы;
- модуль мониторинга сетевой активности серверов подразделений Узкомгосрезерв администратора системы.



4.1.1.2. Перечень сторонних ИС, с которыми должно обеспечено взаимодействие

В связи с тем, что СЭД — это внутренняя система Заказчика для ведения внутреннего документооборота, установление взаимодействия со сторонними ИС не требуется.

Однако, при необходимости, программные и технические средства должны позволять установить взаимодействие со сторонними ИС.

4.1.1.3. Требования к режимам функционирования ИС

Должно быть обеспечено функционирование ИС в следующих режимах:

- Штатный режим (непрерывная круглосуточная работа);
- Профилактический режим (для проведения обслуживания, реконфигурации и пополнения новыми компонентами).

Штатный режим должен являться основным режимом функционирования, обеспечивающим выполнение задач ИС. В рамках режима осуществляется штатное взаимодействие подсистем между собой.

Профилактический режим должен использоваться для изменения конфигурации, параметров работы, настроек, управления правами, выполнения регламентного обслуживания программно-технических средств. В сервисном режиме должна быть обеспечена возможность выполнения функции, связанных с реконфигурацией, конвертированием и архивированием баз данных подсистем.

Пользователи должны работать с базой данных Системы в диалоговом режиме.

Система должна быть предназначена для постоянной и круглосуточной работы пользователей.

Серверы баз данных (архивов) и критического информационного ресурса должны работать в непрерывном круглосуточном режиме, кроме периодов проведения операций копирования данных, ремонтных (восстановительных) или профилактических работ.

Режим функционирования Системы должен обеспечивать выполнение автоматизированных операций по требованию пользователя с задержкой доступа к функционалу

Системы не более 10 секунд, при условии выполнения требований к скорости каналов связи (не ниже 2 Мбит/с).

4.1.1.4. Перечень и описание сценариев использования ИС

Перечень основных сценариев использования в ИС приведен в таблице ниже.

Идентификационный номер	Наименование сценария использования	Действующие лица	Тип сценария
C1	Регистрация документа	Сотрудник Канцелярии, СЭД	Основной
C2	Создание резолюции	Руководитель, Исполнитель, СЭД	Основной
C3	Отметка исполнения документа	Исполнитель, СЭД, Контролирующее лицо	Основной
C4	Продление срока исполнения документа	Исполнитель, СЭД, Контролирующее лицо	Основной

Сценарий использования «C1. Регистрация документа»: Регистрация документа в системе.

Условия запуска: Пользователь осуществил вход в систему и желает зарегистрировать документ.

Основное действующее лицо: Пользователь, на которого возложена обязанность приема и регистрации документов (сотрудник канцелярии), Система СЭД.

Порядок выполнения сценария:

- 1) Пользователь открывает новую форму регистрации и заполняет данные;
- 2) СЭД фиксирует действия пользователя;
- 3) СЭД подгружает необходимые справочники для регистрации документа;
- 4) СЭД генерирует и присваивает уникальный регистрационный номер документу;
- 5) СЭД устанавливает текущую дату регистрации;
- 6) Пользователь загружает электронный образ документа в систему;
- 7) Пользователь сохраняет регистрационную карточку в системе;
- 8) СЭД сохраняет регистрационную карту в базе;
- 9) Пользователь направляет документ на рассмотрение руководству.

Временной регламент выполнения сценария:

- 1) Время сохранения заполненной формы не должен превышать 1 секунды.
- 2) Время сообщения об ошибках не должен превышать 1 секунды.

Входные данные:

При регистрации входящей документации

1. Исходящий номер документа
2. Дата документа
3. Кол-во приложений и страниц
4. Вид документа
5. Корреспондент (Организация)
6. Срок
7. Количество листов в документе
8. Форма документа
9. Литер (шифр)
10. Краткое содержание
11. Поручение вышестоящего органа
12. Подшить к папке (если нужна привязка к другому документу)

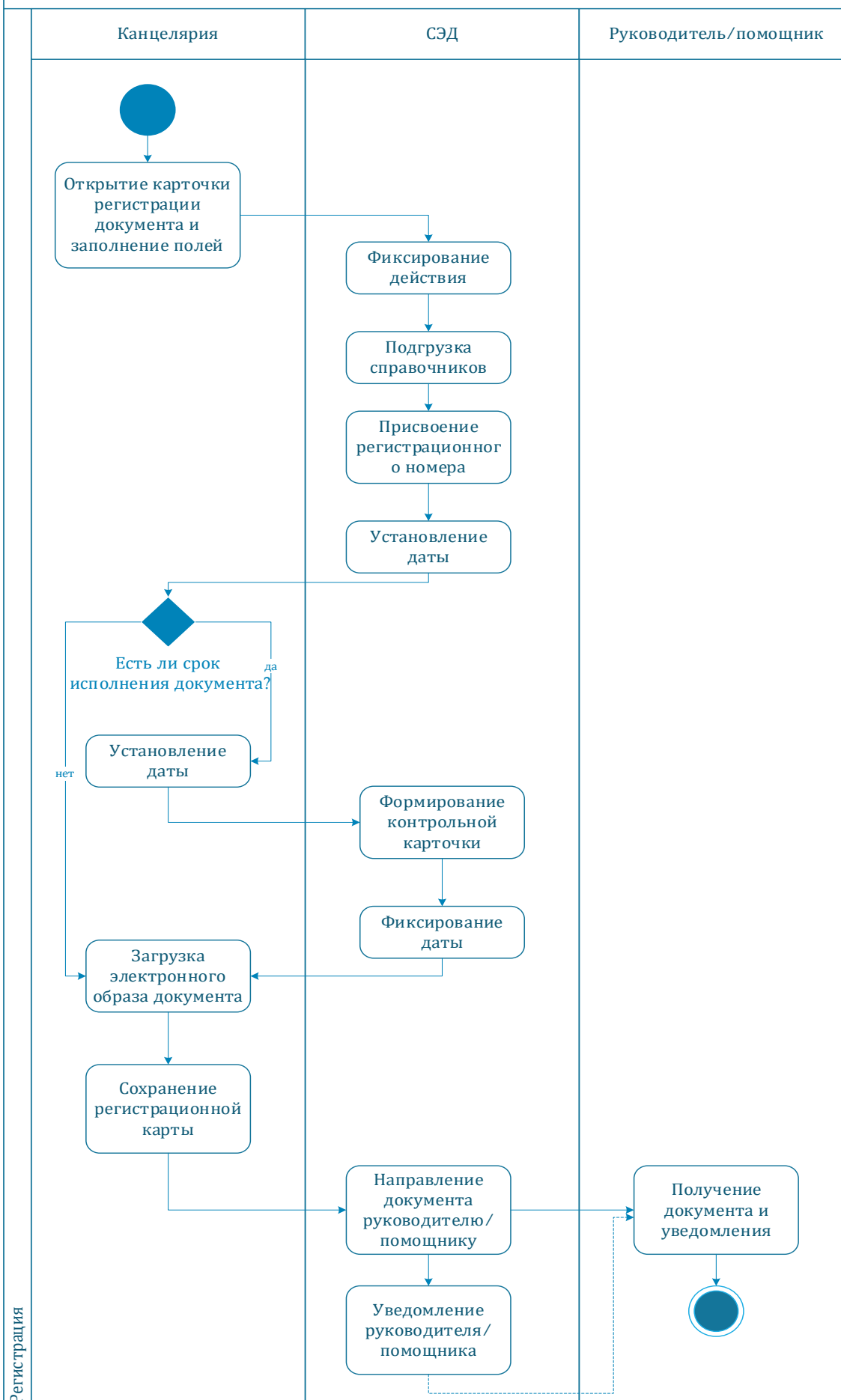
При регистрации исходящей документации

1. Номер бланка (при необходимости)
2. Тип бланка (при необходимости)
3. Вид документа
4. Номер дела
5. Подразделение
6. Автор
7. Краткое содержание
8. Количество листов в документе
9. Литер (шифр)
10. Способ отправки
11. Приложения, стр.
12. Подшить к папке (если нужна привязка к другому документу)
13. Электронный формат документа

Выходные данные:

1. Регистрационный номер
2. Регистрационная дата
3. Регистрационная карточка документа

С.1.Регистрация документа



Сценарий использования «С2. Создании резолюции»: Вынесение резолюции документу помощником или руководителем(начальником).

Условия запуска: Документ зарегистрирован в системе.

Основное действующее лицо: Помощник/Руководитель (Пользователь), Система СЭД, Исполнитель.

Порядок выполнения сценария:

- 1) Пользователь выбирает документ и создает резолюцию к нему
- 2) СЭД фиксирует действия пользователя;
- 3) СЭД подгружает необходимые справочники;
- 4) СЭД подгружает список сотрудников/исполнителей;
- 5) Пользователь выбирает исполнителя/соисполнителей;
- 6) Пользователь вводит поручение или выбирает из справочника;
- 7) Пользователь устанавливает срок исполнения;
- 8) Пользователь отправляет поручение исполнителям;
- 9) СЭД направляет поручение исполнителям и уведомляет их;
- 10) СЭД фиксирует срок исполнения документа;
- 11) Исполнитель получает уведомление и поручение.

Временной регламент выполнения сценария:

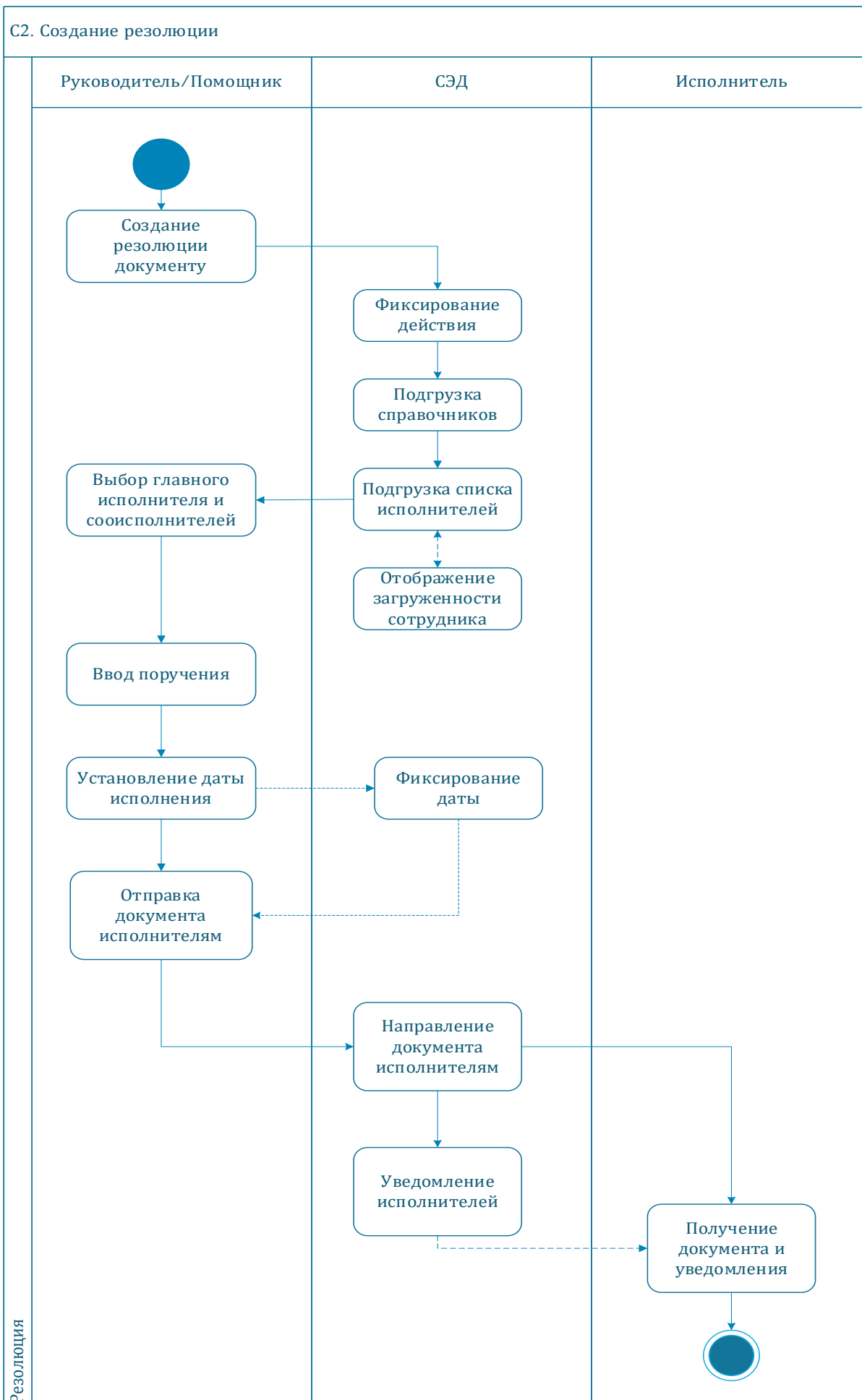
- 1) Время сохранения заполненной формы не должен превышать 1 секунды.
- 2) Время сообщения об ошибках не должен превышать 1 секунды.

Входные данные:

1. Поручение
2. Исполнители
3. Соисполнители
4. Срок исполнения

Выходные данные:

1. Резолюция



Сценарий использования «С3. Отметка исполнения документа»: Отметка итогов выполнения поручения.

Условия запуска: Документ зарегистрирован в системе и имеет исполнителей.

Основное действующее лицо: Исполнитель (Пользователь), СЭД, Контролирующее лицо

Порядок выполнения сценария:

- 1) Пользователь открывает исполненный документ;
- 2) СЭД фиксирует действия пользователя;
- 3) Пользователь прикрепляет файл документа об исполнении и отправляет на рассмотрение Контролирующему лицу;
- 4) СЭД фиксирует дату и время отправки исполнения;
- 5) СЭД направляет документ Контролирующему лицу и уведомляет его;
- 6) Контролирующее лицо получает уведомление и исполненный документ;
- 7) Контролирующее лицо проверяет исполнение;
- 8) Контролирующее лицо снимает с контроля документ;
- 9) СЭД фиксирует снятие с контроля;
- 10) СЭД уведомляет исполнителя.

Временной регламент выполнения сценария:

- 1) Время сохранения заполненной формы не должен превышать 1 секунды.
- 2) Время сообщения об ошибках не должен превышать 1 секунды.

Входные данные:

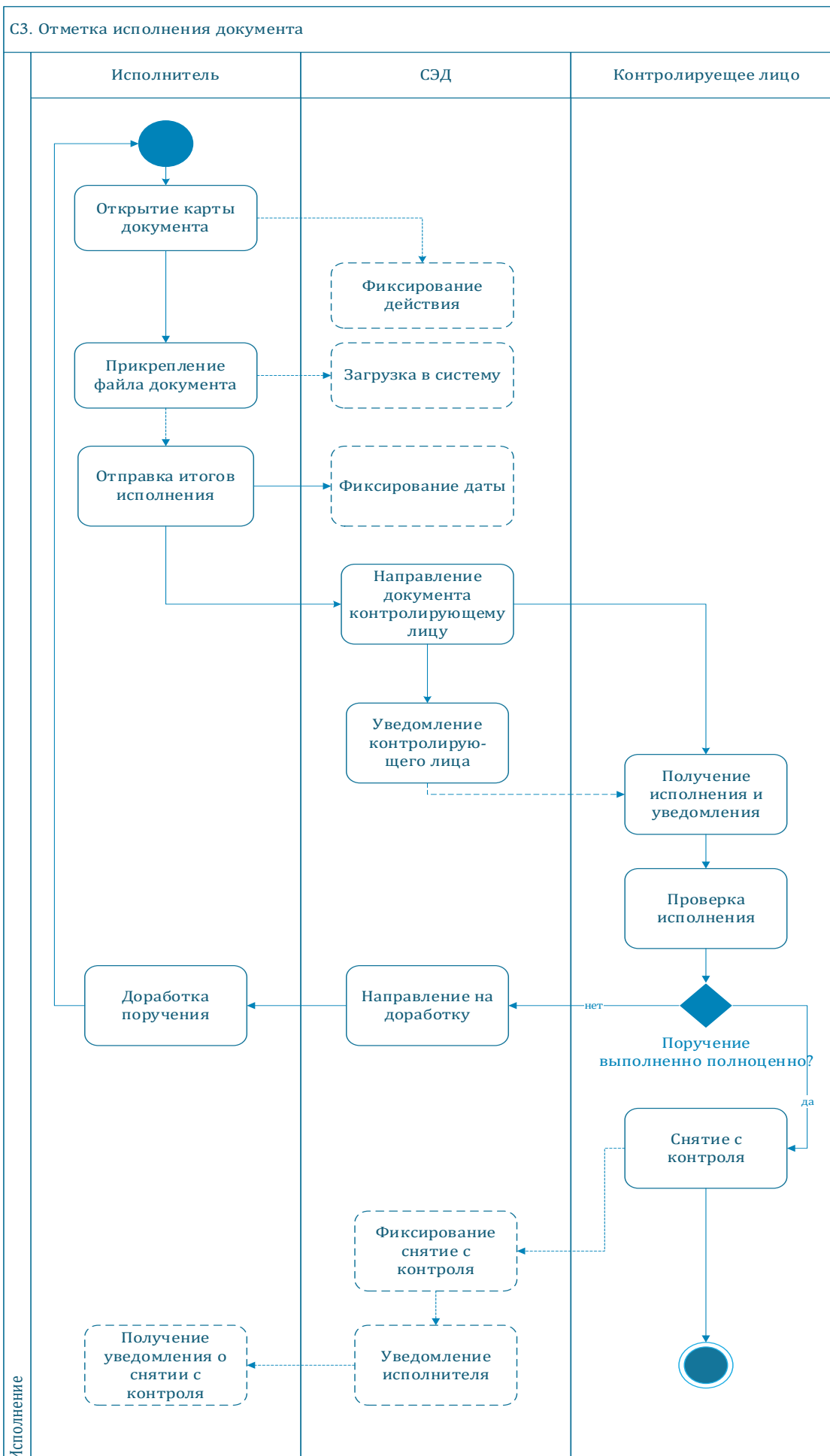
1. Файл документа
2. Комментарии/замечания к документу

Выходные данные:

1. Дата и время снятия с контроля

Расширения

- 8.1. Контролирующее лицо отправляет исполнение на доработку
- 8.2. Исполнитель получает документ на доработку



Сценарий использования «С4. Продление срока исполнения документа».

Условия запуска: Документ зарегистрирован в системе, имеет исполнителей и срок исполнения.

Основное действующее лицо: Исполнитель (Пользователь), СЭД, Контролирующее лицо

Порядок выполнения сценария:

- 1) Пользователь открывает исполненный документ;
- 2) СЭД фиксирует действия пользователя;
- 3) Пользователь формирует запрос о продлении исполнения документа и отправляет на рассмотрение Контролирующему лицу;
- 4) СЭД фиксирует дату и время отправки запроса;
- 5) СЭД направляет запрос Контролирующему лицу и уведомляет его;
- 6) Контролирующее лицо получает уведомление и запрос
- 7) Контролирующее лицо продлевает срок исполнения;
- 8) СЭД фиксирует продление срока исполнения;
- 9) СЭД уведомляет исполнителя.

Временной регламент выполнения сценария:

- 1) Время сохранения заполненной формы не должен превышать 1 секунды.
- 2) Время сообщения об ошибках не должен превышать 1 секунды.

Входные данные:

1. Причины продления срока

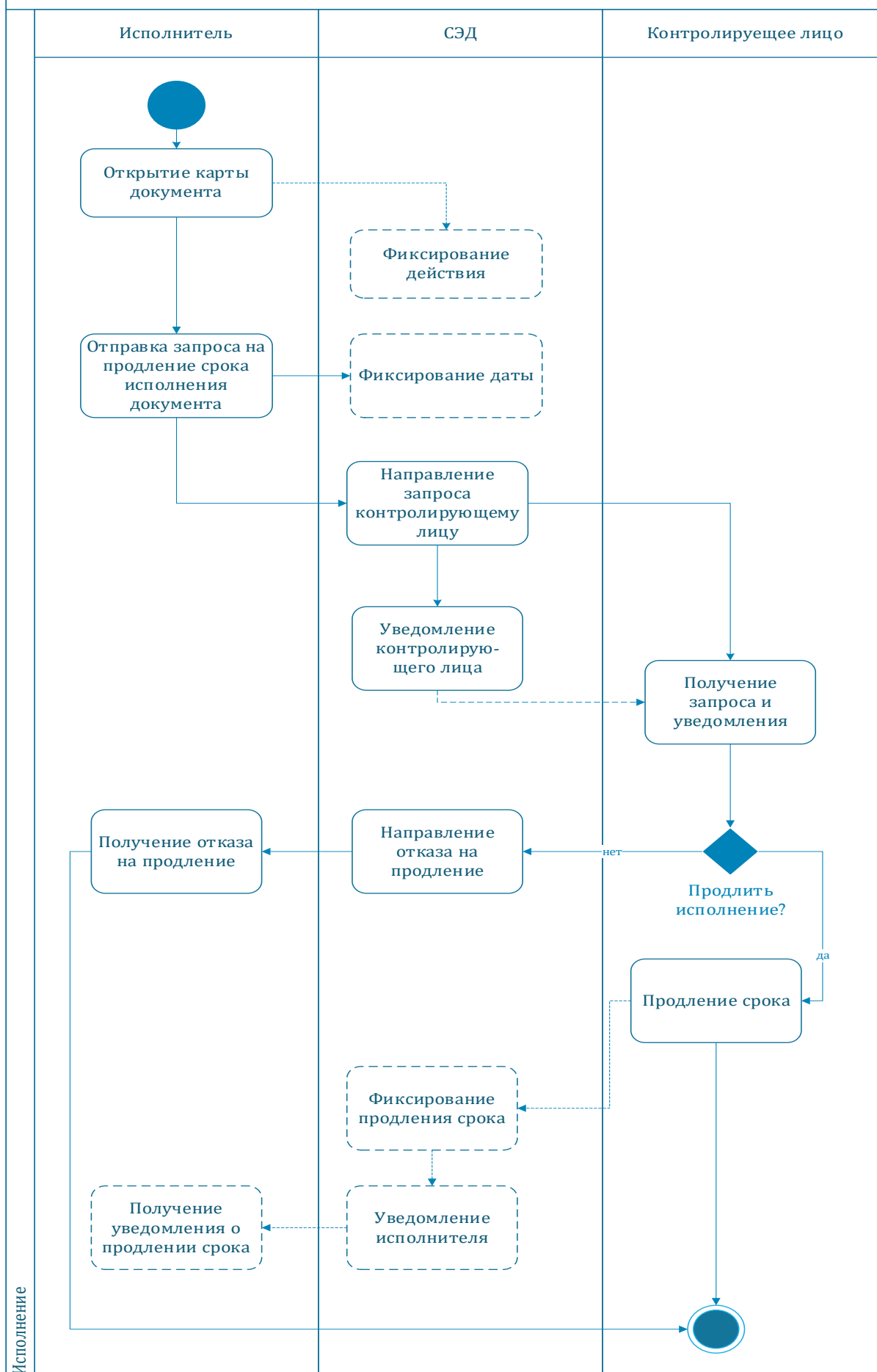
Выходные данные:

1. Срок выполнения поручения (новый)

Расширения

- 7.1. Контролирующее лицо отклоняет продление срока

С4. Продление срока исполнения документа



4.1.1.5. Требования по диагностированию ИС

ИС должна предоставлять инструменты диагностирования основных процессов ИС, и мониторинг их выполнения. Компоненты должны предоставлять удобный интерфейс для возможности просмотра диагностических событий, мониторинга процесса выполнения программ.

При возникновении аварийных ситуаций либо ошибок в программном обеспечении, диагностические инструменты должны позволять сохранить полный набор информации, необходимой разработчику для идентификации проблемы.

4.1.1.6. Перспективы развития, модернизации ИС

При создании Системы должны быть предусмотрены перспективы развития и возможности последующей модернизации в ходе появления новых задач по автоматизации рабочих процессов структурных подразделений Заказчика, а также появления новых тенденций и прогрессивных новаций в области информационных технологий.

Должны быть предусмотрены следующие направления развития:

- обеспечение Системой возможности расширения числа пользователей;
- расширение функциональности Системы в процессе ее сопровождения (изменение функциональности эксплуатируемых подсистем и внедрение новых подсистем);
- масштабируемость Системы, с возможностью адаптации к новым требованиям заказчика;
- обновление и модернизация инфраструктурного программного обеспечения, таких как:
- операционная система;
- сервер приложений;
- СУБД и применение новых СЗИ;
- готовность Системы к возможной перспективной интеграции со смежными информационными системами.

4.1.2. Требования к взаимодействию со сторонними информационными системами

4.1.2.1. Общие требования к взаимодействию

Взаимодействие Системы со сторонними информационными системами должна быть реализована согласно требованиям О'zDSt 2590:2012 Информационная технология. Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы.

При взаимодействии ИС, должна осуществляться идентификация и аутентификация информационных систем по идентификатору (коду) и паролю условно-постоянного действия длиной не менее восьми буквенно-цифровых символов или с использованием криптографических методов.

При разработке веб-сервиса должны быть соблюдены следующие особые условия и ограничения:

- все описания электронных сервисов и описания схем данных XSD должны создаваться в кодировке UTF-8 или UTF-16;
- в описаниях веб-сервиса запрещены циклические ссылки между описаниями двух и более сервисов;
- все описания электронных сервисов должны содержать развернутую структуру входящих и выходящих параметров.

Меры по защите информации должны обеспечивать достижение трех основных свойств информации:

Целостности – информация должна быть достоверной и точной, а также защищена от возможных непреднамеренных и злоумышленных искажений;

Доступности – информация и соответствующие автоматизированные службы должны быть доступны, готовы к обслуживанию всегда, когда в них возникает необходимость у имеющего право доступа персонала;

Конфиденциальности – конфиденциальная информация должна быть доступна только тому, кому она предназначена.

Состав и форматы передаваемых данных должны быть уточнены и утверждены на этапе технического проектирования. Требования к взаимодействию со сторонними ИС должны быть оформлены в виде технологической инструкции.

4.1.2.2. Представление исходящего электронного документа в виде XML-документа для передачи между различными СЭД

Исходящий электронный документ для передачи в виде файла между различными СЭД должен удовлетворять соответствующим правилам XML (XML-документ): иметь установленную структуру, заданный состав элементов и их атрибутов.

Исходящий электронный документ (файл) и все его составные части могут быть подписаны ЭЦП и/или зашифрованы, после чего формируется XML-документ для передачи в другую СЭД.

Исходящий электронный документ в Системе в виде XML-документа должен соответствовать государственному стандарту O'z DSt 1270:2009.

4.1.3. Требования к численности и квалификации персонала ИС и режиму его работы

Персонал ИС можно разделить на две категории:

Основной персонал – пользователи, выполняющие эксплуатацию ИС в своей деятельности.

Персонал технического обслуживания - администраторы и персонал технического обслуживания.

4.1.3.1. Требования к численности персонала (пользователей) ИС

Штатный состав персонала, эксплуатирующая ИС, должен формироваться на основании нормативных документов Республики Узбекистан и Трудового кодекса.

Система должна обеспечить одновременную и бесперебойную работу до 5 тыс. пользователей.

Обслуживание Системы должно осуществляться персоналом, ответственным за внедрение информационно-коммуникационных технологий Заказчика.

В состав персонала, эксплуатирующего Систему, должны входить системные и администраторы локальной сети, администраторы по информационной безопасности, а также специалисты по линиям связи и аппаратной части ТСИ.

При формировании требований к персоналу Системы, необходимо учитывать круглосуточный режим работы Системы, а также требования положения о порядке прохождения военной службы гражданами Республики Узбекистан и трудового законодательства Республики Узбекистан.

Функционирование Системы должно включать в себя следующие процессы:

- эксплуатация Системы;
- системно-техническое обслуживание;
- поддержка прикладного программного обеспечения.

Эксплуатацию Системы должны осуществлять сотрудники, отвечающие за текущее делопроизводство, и администратор, зарегистрированные в Системе как пользователи с определенными правами доступа.

Системно-техническое обслуживание и поддержка прикладного программного обеспечения должны обеспечиваться:

1. Администратором Системы (администратором по ИБ);
2. Администратором локальной сети;
3. Системным администратором.

4.1.3.2. Требования к квалификации персонала, порядку его подготовки и контроля знаний и навыков.

Основные пользователи ИС должны обладать базовыми знаниями и навыками по работе с персональными электронными вычислительными машинами и интернет-браузером, уметь

выполнять типовые операции по вводу данных в стандартные формы, просмотру данных по стандартным запросам и созданию стандартных документов.

Персонал технического обслуживания должен владеть общими принципами построения ИС, конфигурированием и настройкой программно-технического комплекса ИС, знать настройку программной и аппаратной части, обладать знаниями и умением классифицировать и устранять возникающие ошибки. Персонал, эксплуатирующий Систему, должен владеть навыками выполнения возложенных на них задач, иметь навыки администрирования ОС семейства LINUX, WINDOWS, средств виртуализации, СУБД и сетевых технологий.

Персонал (пользователи) должен проходить обязательную общую и специальную подготовку для работы с ИС и средствами вычислительной техники.

Общая подготовка должна включать в себя получение или совершенствование навыков работы с общераспространенным программным обеспечением (офисное ПО и оболочки персональных компьютеров).

Специальная подготовка должна включать в себя получение навыков работы с данной ИС.

Персонал (пользователи) ИС должны пройти обучение по специальной и общей подготовке персонала ИС с обязательным контролем знаний и навыков.

Для проведения контроля знаний и навыков по работе с ИС должны быть разработаны соответствующие методические и регламентирующие документы.

Состав и перечень необходимых навыков общей и специальной подготовки, а также порядок контроля знаний разрабатываются на этапе технического проекта и согласовываются протоколами заказчиком.

4.1.3.3. Требуемый режим работы персонала ИС

Требования к режиму работы персонала определяются правилами внутреннего распорядка.

ИС эксплуатируется на персональных компьютерах, поэтому требования к организации труда и режима отдыха при работе с ней должны устанавливаться, исходя из требований к организации труда и режима отдыха при работе с этим типом средств вычислительной техники.

4.1.4. Показатели назначения

4.1.4.1. Значения параметров, характеризующие степень соответствия ИС по назначению

ИС должна поддерживать работу пользователей, находящихся на территориально разобщенных объектах.

ИС должна формировать единое информационное пространство, в котором взаимодействие процессов и пользователей обеспечивается за счет общих информационных объектов.

Должна обеспечиваться возможность перенастройки ИС при изменении нормативно-правовой базы.

Должна обеспечиваться возможность увеличения количества одновременно работающих пользователей.

Должно быть обеспечено поэтапное наращивание как производительности, так и функционального состава ИС.

Должен быть реализован принцип открытой архитектуры построения ИС, обеспечивающий возможность встраивания и взаимодействия с любыми другими ИС. ИС должна иметь открытые интерфейсы для развития и интеграции.

Время ответа на действие пользователя в Системе не должно превышать 5 секунд.

4.1.4.2. Вероятностно-временные характеристики, при которых сохраняется целевое назначение ИС

Период накопления данных в системе до 5 лет, после установленного срока ИС должна позволить архивацию данных.

Период накопления архивных данных устанавливается соответствующим внутренним положением Заказчика.

Минимально допустимый срок эксплуатации ИС при этом должен быть не менее 15 лет.

4.1.5. Требования к надежности

Надежность ИС определяется надежностью функциональных модулей, общего программного обеспечения, комплексов технических и инженерных средств.

4.1.5.1. Состав и количественные значения показателей надежности для ИС в целом или её подсистем

Должно обеспечиваться:

- Сохранение работоспособности ИС при отказе или выходе из строя по любым причинам одного из компонентов комплекса технических средств или телекоммуникационной подсистемы;
- Сохранение всей накопленной на момент отказа или выхода из строя информации при отказе двух и более одинаковых по назначению компонентов ИС не зависимо от их назначения, с последующим восстановлением после проведения ремонтных и восстановительных работ функционирования ИС.

Должны быть обеспечены два уровня надежности ИС:

1. Уровень сохранения работоспособности;
2. Уровень сохранности информации.

Показатели надежности должны обеспечивать возможность эффективного выполнения функциональных задач ИС.

Показатели надежности включают:

- Среднее время между выходом из строя отдельных компонентов ИС;
- Среднее время на обслуживание, ремонт или замену вышедшего из строя компонента;
- Среднее время на восстановление работоспособности ИС.

Показатели надежности ИС должны достигаться комплексом организационно-технических мер обеспечивающих доступность ресурсов, их управляемость и обслуживаемость.

Технические меры по обеспечению надежности должны предусматривать:

- Резервирование критически важных компонентов и данных ИС и отсутствие единой точки отказа;
- Использование технических средств с избыточными компонентами и возможностью их горячей замены;
- Конфигурирование используемых средств и применение специализированного ПО, обеспечивающего высокую доступность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок пользователей, а также персонала службы эксплуатации при эксплуатации и проведении работ по обслуживанию комплекса технических средств ИС, минимизацию времени ремонта или замены вышедших из строя компонентов.

В целом, надежность аппаратно-программного обеспечения должна обеспечивать выполнение задач ИС с временем однократного простоя не более 30 мин и суммарным временем простоя не более 24 часов в год.

4.1.5.2. Перечень аварийных ситуаций, по которым должны быть регламентированы требования к надежности, и значения соответствующих показателей

Сохранение работоспособности обеспечивается при возникновении локальных отказов компонентов ИС:

- Отказ рабочего места пользователя;
- Отказ линии связи или сегмента ЛВС;
- Отказ центра обработки данных (ЦОД).

Полный перечень отказов и их критериев уточняется Исполнителем на стадии рабочей документации и согласовывается протоколом с Заказчиком.

Сохранность информации в Системе должна обеспечиваться при следующих аварийных ситуациях:

нарушения электропитания:

провалы напряжения - кратковременные понижения при резком увеличении нагрузки в электрической сети;

высоковольтные импульсы - кратковременные значительные увеличения напряжения;

полное отключение электроэнергии - полное отключение электроэнергии вследствие аварий, перегрузок;
слишком большое напряжение - кратковременное увеличение напряжения в сети;
нестабильность частоты питающего напряжения.
нарушение или выход из строя каналов связи локальной сети Сервиса;
полный или частичный отказ технических средств ИС, включая сбои и отказы накопителей на жестких магнитных дисках;
сбой общего или специального программного обеспечения ИС;
ошибки в работе технического персонала;
выход из строя комплекса технических средств за счет аварий техногенного характера - повреждение внешних каналов связи, нарушение ИС электропитания здания, повреждение ИС водоснабжения здания и т.д.;

выход из строя элемента сетевой инфраструктуры ИС;
выход из строя одиночного сервера;
выход из строя одиночного дискового массива сервера;
выход из строя диска сервера;
выход из строя процессора сервера;
выход из строя банка памяти сервера;
выход из строя сетевого адаптера сервера;
выход из строя внутреннего источника питания сервера;
нарушение логической целостности информации, хранящейся на диске сервера.
выход из строя диска ИС хранения данных;
выход из строя контроллера управления ИС хранения данных;
физическое повреждение или обрыв одной линии связи ИС хранения данных и сервера баз данных;

4.1.5.3. Требования к надежности технических средств и программного обеспечения

К критически важным ресурсам ИС относятся сетевая инфраструктура серверных комплексов.

Технические средства серверного сегмента ЛВС и серверов СУБД должны обеспечивать диагностирование работоспособности оборудования и ПО, избыточность аппаратного обеспечения, возможность горячей замены компонентов активного сетевого оборудования и аппаратного обеспечения сервера, возможность резервирования путей взаимодействия серверов.

Надежность активного сетевого оборудования должна обеспечивать время однократного простоя не более 15 мин, суммарного времени на регламентное обслуживание не более 48 часов в год.

Надежность серверов СУБД должна обеспечивать время однократного простоя не более 30 мин, суммарного времени на регламентное обслуживание не более 48 часов в год.

Время на восстановление работоспособности отдельных компонентов активного оборудования ЛВС и серверов не должно превышать - 8 часов, в прочих случаях - определяется временем заказа и поставки необходимого оборудования. Время восстановления работоспособности включает время на диагностирование отказа, замену или ремонт оборудования, конфигурирование оборудования и ПО, восстановление данных и тестирование работоспособности оборудования и ПО.

Надежность серверов приложений должна обеспечиваться выбором аппаратной платформы с возможностью горячей замены отдельных компонентов и дублированием процессоров, блоков питания, дисков и сетевых соединений.

Надежность серверов приложений должна обеспечивать время однократного простоя не более 8 часов, суммарного времени на регламентное обслуживание не более 48 часов в год.

Надежность предоставления информационных сервисов серверами приложений должна обеспечиваться резервированием сервисов, настройками клиентских ОС и комплексом организационных мер, обеспечивающих порядок реагирования на нештатные и аварийные ситуации, своевременную синхронизацию данных между основными и резервными серверами и оповещение о возникающих проблемах технических служб ИС.

Система должна обеспечивать доступ к собственным ресурсам в режиме 24/7/365.

4.1.5.4. Требования к методам оценки и контроля показателей надежности на разных стадиях создания ИС

Текущий контроль показателей надежности должен быть организован в процессе эксплуатации ИС за счет анализа работоспособности ЦОД, РЦОД и его подсистем, тестирования переключения подсистем ЦОД, РЦОД на резервные компоненты ЦОД и РЦОД в соответствии с установленным регламентом.

4.1.6. Требования к безопасности

4.1.6.1. Требования безопасности технических средств

При внедрении, эксплуатации и обслуживании технических средств ИС должны выполняться меры электробезопасности в соответствии с «Правилами устройства электроустановок». Аппаратное обеспечение ИС должно соответствовать требованиям пожарной безопасности в производственных помещениях по «Системе стандартов безопасности труда. Пожарная безопасность. Общие требования».

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

При монтаже, наладке, эксплуатации, обслуживании и ремонте технических средств ИС необходимо обеспечить соблюдение требований ИКН 17 2010 УзАСИ «Ведомственные строительные нормы. Проектирование структурированных кабельных систем и локальных вычислительных сетей», РН 45-201:2011 «Технические требования к зданиям и сооружениям для установки средств вычислительной техники», O'z DSt 2875-2014 «Информационная безопасность. Требование к датацентрам. Инфраструктура и обеспечение информационной безопасности», КМК 2.04.17-98 «Электрооборудование жилых и общественных зданий» и ГОСТ 12.1.030-81 (ИС стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление) и правилами устройства электроустановок.

4.1.6.2. Требования к защите информации от несанкционированного доступа

Разработка ИС, должны осуществляться с учетом требований государственных стандартов по защите информации от несанкционированного доступа. Защита информации ИС должна быть установлена согласно требованиям, к классу защищенности 1А по O'z DSt 2814:2014 «Информационная технология. Автоматизированные системы. Классификация по уровню защищенности от несанкционированного доступа к информации».

При этом следует рассмотреть необходимость:

- управления доступом к информации и сервисам, включая требования к разделению обязанностей и ресурсов;
- регистрации значительных событий в контрольном журнале для целей повседневного контроля или специальных расследований;
- проверки и обеспечения целостности жизненно важных данных на всех или избранных стадиях их обработки;
- защиты конфиденциальных данных от несанкционированного раскрытия, в том числе возможное использование средств шифрования данных;
- выполнения требований инструкций и действующего законодательства, а также договорных требований;
- снятия резервных копий с критически важных данных;
- восстановления систем после отказов, особенно для систем с повышенными требованиями к доступности;
- защиты систем от внесения несанкционированных дополнений и изменений;
- представления возможности безопасного управления ИС и их использования сотрудникам;
- проектирование и эксплуатация систем должны соответствовать общепринятым промышленным стандартам обеспечения надёжной защиты, определенным в государственных стандартах и международных правилах управления безопасностью;

– должна обеспечиваться безопасность в среде разработки и рабочей среде, в том числе определены процедуры управления процессом внесения изменений, технический анализ изменений, вносимых в операционную ИС, ограничения на внесение изменений в пакет программ и т.д.

– при внедрении новой ИС руководством должен быть регламентирован процесс утверждения информационных решений.

Для обеспечения защиты ИС могут применяться следующие механизмы безопасности:

Аутентификация пользователей может осуществляться на основе применения одного или нескольких из следующих механизмов безопасности:

- аутентификации на основе паролей;
- использование протоколов запрос-ответ с использованием серверов авторизации;
- аутентификации на основе физического владения идентификатором;
- аутентификации на основе физических свойств пользователя;

Обеспечение конфиденциальности информации может осуществляться на основе применения механизмов:

- пользовательского шифрования блоков данных и файлов;
- проходного шифрования трафика сети;
- отключения/удаления неиспользуемых сервисов операционных систем и общего программного обеспечения;

- использования лицензионных средств защиты, в том числе программного обеспечения;

Обеспечение неотказуемости от переданных электронных документов может осуществляться на основе применения механизмов:

- электронной цифровой подписи;
- ведения журналов приема/передачи электронных документов;
- установления временных меток.

Обеспечение целостности информации и программного обеспечения может осуществляться на основе применения механизмов:

- резервирования/восстановления программного обеспечения и данных;
- физического контроля доступа к техническим средствам;
- отключения/удаления локальных устройств ввода/вывода информации;
- использование антивирусных средств;
- хеширования.

Для обеспечения неизменности программной среды могут быть использованы механизмы контроля целостности программных и информационных файлов. Контроль их целостности может обеспечиваться:

- средствами подсчета контрольных сумм;
- средствами мониторинга динамики значений параметров программных объектов;
- средствами электронной цифровой подписи;
- средствами сравнения критичных ресурсов с их эталонными копиями;
- средствами разграничения доступа.

Контроль доступа к ресурсам может обеспечиваться на основе применения механизмов:

- ведения списков контроля доступа;
- определения матрицы доступа;
- ролевого доступа;
- идентификации;
- использования межсетевого экранирования на пакетном, транспортном и прикладном уровнях;

- использования трансляции сетевых адресов;
- контроль содержимого (e-mail, http, ftp, и т.д.).

Средствами контроля доступа должна обеспечиваться аутентификация пользователя ИС и его авторизация.

Обеспечение доступности ресурсов может осуществляться на основе применения механизмов:

– холодного и горячего резервирования, в том числе реализации катастрофоустойчивой схемы для важнейших программно-аппаратных комплексов;

- кластеризации;
- резервирования программного обеспечения и данных;
- создания резервных источников электропитания;
- назначения приоритетов доступа.

Мониторинг и аудит может проводиться на основе применения механизмов:

- регистрации доступа (чтение, запись, удаление, создание) к данным;
- регистрации запуска процессов;
- регистрации статуса выполненной операции (удачно/неудачно);
- регистрации операций администрирования;
- регистрации изменения привилегий и прав доступа;
- регистрации вывода информации на печать и внешние носители;
- оперативного уведомления об НСД;
- анализа сетевого трафика;
- анализа системной активности;
- регистрации входа (выхода) в ИС.

Средства мониторинга и аудита должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т. п.), которые могут повлечь за собой нарушение политики информационной безопасности и привести к возникновению кризисных ситуаций.

4.1.6.3. Требования к обеспечению информационной безопасности системы с применением электронно-цифровой подписи

Электронная цифровая подпись является одним из значимых и эффективных инструментов обеспечения высокого уровня защищённости электронных документов, который позволяет обеспечить требуемый высокий уровень информационной безопасности.

Электронная цифровая подпись — это реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки. ЭЦП формируется в результате преобразования информации с использованием средств криптографической защиты информации (СКЗИ) и позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. Протоколирование действий пользователей, криптографическое шифрование и применение ЭЦП при согласовании документов полностью исключает вероятность несанкционированного доступа.

В Системе должна применяться ЭЦП в соответствии с требованиями Законов Республики Узбекистан «Об электронной цифровой подписи» и «Об электронном документообороте».

Формирование и проверка ЭЦП в Системе должна осуществляться в соответствии с государственным стандартом O'z DSt 1092:2009.

Сертификаты ЭЦП Системы должны принадлежать Центру регистрации ключей ЭЦП по выбору Заказчика и Исполнителя.

При проверке ЭЦП должны проверяться:

- подлинность ЭЦП - отсутствие искажений в подписанном документе и подтверждение принадлежности ЭЦП пользователю Системы, сформировавшему ЭЦП;
- действительность сертификата открытого ключа ЭЦП в момент формирования ЭЦП.

Проверка действительности сертификата открытого ключа ЭЦП должна производиться в момент формирования ЭЦП путем проверки:

- срока действия сертификата открытого ключа ЭЦП;
- проверки статуса сертификата (действителен, приостановлен, аннулирован) путем проверки сертификата в списке отозванных сертификатов.

Модуль ЭЦП осуществляет:

- Подпись исходящих документов;
- Подпись входящих документов;
- Подпись внутренних документов;
- Подпись приказов и распоряжений;
- Подпись резолюций, отметок об исполнении, хода исполнения;

- Проверку достоверности подписей (если ЭЦП под документом верна, это значит, что документ действительно подписан отправителем и в текст документа не внесено никаких изменений, в противном случае будет выдаваться сообщение, что сертификат отправителя не является действительным).

В подпись записывается следующая информация:

- имя файла открытого ключа подписи;
- информация о лице, сформировавшем подпись;
- дата формирования подписи.

В системе электронного документооборота будет организовано хранилище сертификатов открытых ключей.

4.1.6.4. Требования по сохранности информации при авариях

Используемые при развертывании ИС аппаратные и системные платформы ЦОД и РЦОД должны обеспечивать сохранность и целостность информации при полном или частичном отключении электропитания, аварии сетей телекоммуникации, полном или частичном отказе технических средств, на которых эксплуатируется ИС.

Сохранность информации должна быть обеспечена в случае:

- отключения электропитания;
- отказа одного или нескольких серверов приложений ИС;
- отказа одного или нескольких серверов баз данных ИС;
- одного или нескольких хранилищ данных ИС;
- временного отказа линий связи.

Все аварийные ситуации должны обрабатываться программно с корректной обработкой ситуации (завершение транзакций, закрытие файлов и т.п.), без потери обрабатываемой информации.

В случае возникновения аварии или сбоя в процессе выполнения пользовательских задач должно быть обеспечено восстановление базы данных до состояния на момент последней завершенной ИС транзакции.

В случае повреждения журналов транзакций СУБД должно обеспечиваться восстановление состояния ИС на момент создания последней резервной копии данных, но не более, чем за сутки до момента сбоя.

4.1.6.4 Требования к защите от влияния внешнего воздействия

Применительно к программно-аппаратному окружению ИС предъявляются следующие требования к защите от влияния внешних воздействий.

Требования к радиоэлектронной защите:

- электромагнитное излучение радиодиапазона, возникающее при работе электробытовых приборов, электрических машин и установок, приёмопередающих устройств, эксплуатируемых на месте размещения программно-аппаратного комплекса ИС, не должны приводить к нарушениям работоспособности подсистем.

Требования по стойкости, устойчивости и прочности к внешним воздействиям:

- ИС должна иметь возможность функционирования при колебаниях напряжения электропитания;

- ИС должна иметь возможность функционирования в диапазоне допустимых температур окружающей среды, установленных изготовителем аппаратных средств.

- ИС должна иметь возможность функционирования в диапазоне допустимых значений влажности окружающей среды, установленных изготовителем аппаратных средств.

- ИС должна иметь возможность функционирования в диапазоне допустимых значений вибраций, установленных изготовителем аппаратных средств.

4.1.7. Требования к эргономике и технической эстетике

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав ИС должно осуществляться посредством визуального графического интерфейса. Интерфейс ИС должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм. Навигационные

элементы должны быть выполнены в удобной для пользователя форме. Средства редактирования информации должны удовлетворять принятым соглашениям в части использования функциональных клавиш, режимов работы, поиска, использования оконной ИС. Ввод-вывод данных ИС, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме.

Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям ИС. Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», то есть управление ИС должно осуществляться с помощью набора экранных меню, кнопок, значков и т. п. элементов. Клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм. Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений) должны быть на государственном или русском языке (язык выбирается пользователем самостоятельно).

ИС должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях ИС должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных. Экранные формы должны проектироваться с учетом требований унификации:

все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;

для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы;

внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов.

4.1.8. Требования к патентной и лицензионной чистоте

По всем техническим и программным средствам, применяемым в системе, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота.

ИС является интеллектуальной собственностью Исполнителя. Заказчику передаются исключительные права на использование ИС.

4.1.9. Требования по стандартизации и унификации

Разработка ИС должна быть реализована с использованием стандартных и унифицированных методов разработки программных средств.

Унификация информационной базы (нормативно-справочной информации, входных и выходных документов, описаний информационных объектов и правил задания и представления реквизитов описания этих объектов) должна обеспечивать целостность и однозначной взаимосвязи данных в базе данных ИС.

В ИС необходимо задействовать использование классификаторов. Использование единой ИС классификации и кодирования информации в ИС должно устанавливать общие требования к формированию и унификации информационных ресурсов, предназначенных для работы с ИС на всех уровнях взаимодействия.

4.2. Требования к функциям (задачам), выполняемым ИС

Система должна обеспечивать выполнение перечисленных ниже функций в рамках решений соответствующих задач, которые объединены в указанные ниже требования.

Приведенный перечень функций (задач) должен определять все функциональное наполнение СЭД и, возможно, будет дополнительно детализирован на стадиях техно-рабочего проектирования Системы.

4.2.1. Общие требования к делопроизводственным функциям

Рис.1 отображает обработку входящей корреспонденции Системы, которая начинается с регистрации и осуществляется по двум источникам данных:

- 1) прием и регистрация документа (подготовленного, поступившего и распорядительного) в электронном виде;
- 2) регистрация документа (подготовленного, поступившего и распорядительного) в бумажном виде.

После заполнения необходимых реквизитов и прикрепления отсканированного документа, входящий документ регистрируется и сохраняется в журнале регистрации. Зарегистрированный документ отправляется руководителю (или помощнику руководителя для подготовки проекта резолюции) на рассмотрение и для наложения резолюции. Ознакомившись с деталями и реквизитами зарегистрированного документа, руководитель проставляет резолюцию (руководитель имеет право вносить изменения в проект резолюции) выбрав необходимых получателей (по схеме заместителей руководителя).

В свою очередь ответственные получатели (заместители руководителя) резолюции, после ознакомления всех деталей, формируют собственную резолюцию с выбором ответственных исполнителей или подразделений, сроков и добавлением важных замечаний для резолюции и направляют исполнителям и контролирующему лицу. При необходимости контролирующее лицо делает запрос руководителю на изменение резолюции и добавление других исполнителей через Систему. После получения поручения исполнитель, на основании поступившего документа, готовит проект внутреннего или исходящего документа (ответное письмо, приказ или документ на основании приказа) и направляет его для ознакомления контролирующему лицу и утверждения руководителю. Утвержденный руководителем документ снимается с контроля (если была создана контрольная карточка к резолюции) и направляется для регистрации как исходящий документ.

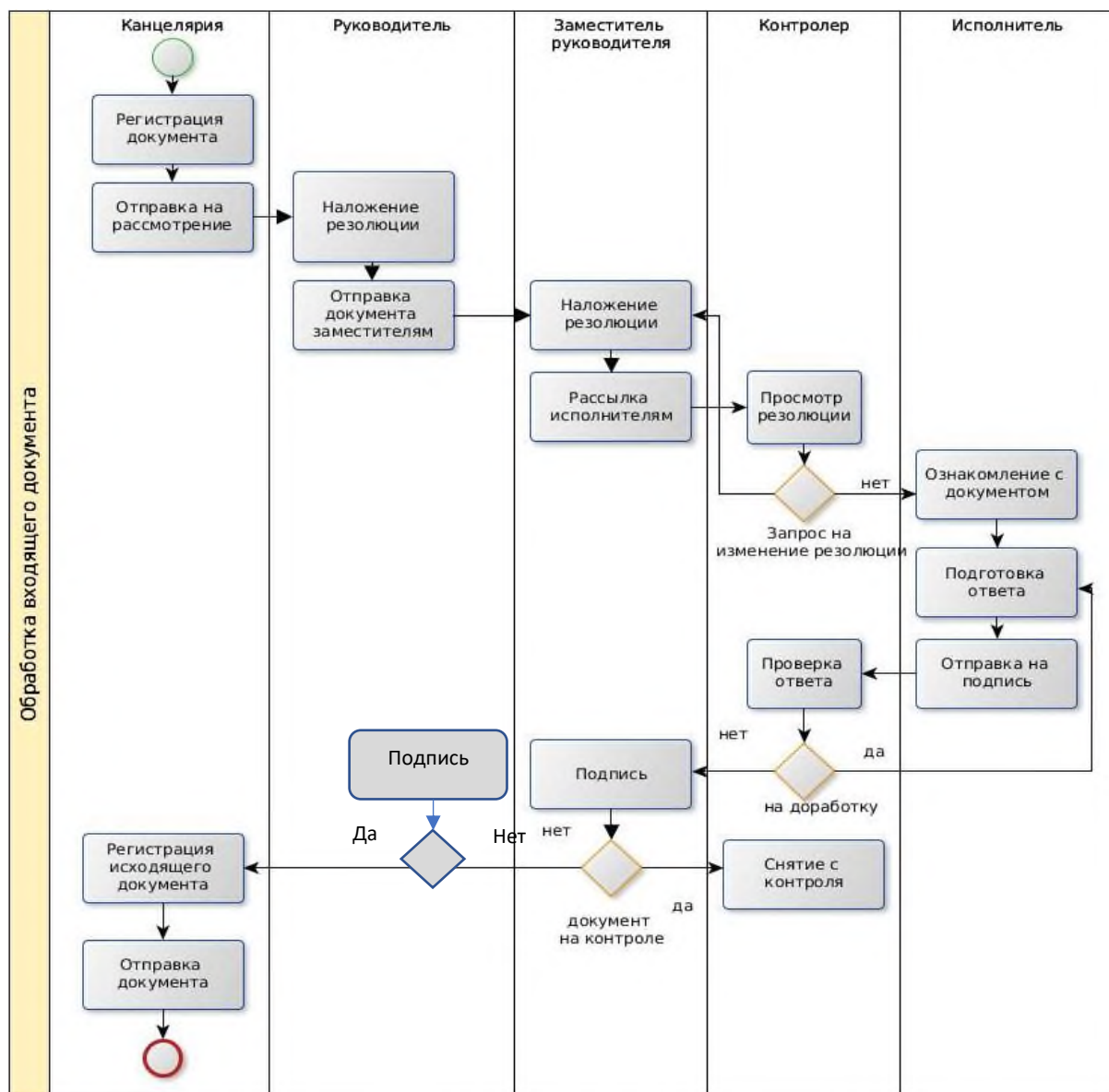


Рис.1. Принципиальная схема обработки входящего документа в Системе

Рис.2 отображает исполнение задач, резолюции и контрольных карточек в Системе. После получения поручения исполнитель, на основании поступившего документа, готовит проект внутреннего или исходящего документа (ответное письмо, приказ или документ на основании приказа) и направляет его для ознакомления контролирующему лицу. При наличии недостатков в проекте, документ направляется на доработку исполнителю. После доработки отправляется на утверждение руководителю и на снятие с контроля.

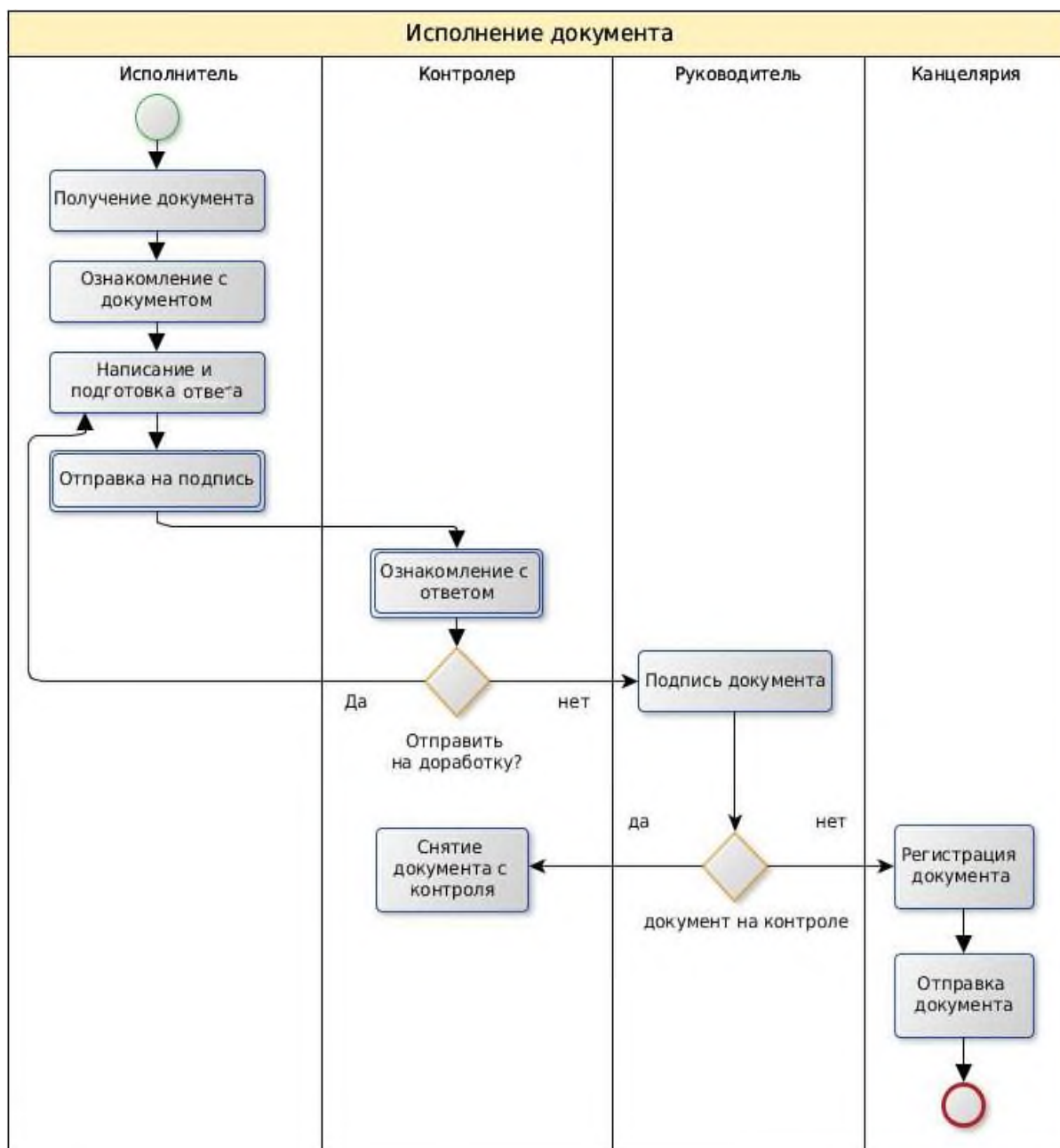


Рис.2. Принципиальная схема исполнения документа в Системе

Система должна обеспечивать автоматизацию следующих делопроизводственных функций:

- централизованная и децентрализованная регистрация входящей, и исходящей корреспонденции;
- установление задания на корреспонденцию с указанием действия: на исполнение, на ознакомление, на согласование, на подпись, на доклад;
- выдача резолюции руководства на входящую корреспонденцию;
- согласование документов;
- осуществление централизованного контроля исполнения приоритетных документов с заведением на них контрольных карточек;
- осуществление контроля исполнения заданий, резолюций руководства и контрольных карточек;
- поиск документов в разделе по любому набору реквизитов регистрационно-контрольной карточки электронного документа;
- отправка документов, формирование реестров рассылки в т.ч. в бумажном виде;

- регламентация прав доступа в базу данных, а также определение набора делопроизводственных функций допустимых для конкретного пользователя;
- возможность организации совместной работы над одним документом с указанием конкретных заданий каждому сотруднику.

4.2.2. Требования к функциям контроля исполнения

Контроль осуществляется руководителем, его заместителями в соответствии с распределенными между ними обязанностями, а также сотрудником канцелярии. Контролирующее лицо имеет право на продление срока контрольной карточки при согласовании с руководителем. Им же осуществляется контроль исполнения контрольной карточки и при необходимости делается запрос руководителю на изменение резолюции и добавление других исполнителей через Систему.

Обязательному контролю подлежат: указы, постановления, распоряжения Президента Республики Узбекистан, постановления, распоряжения, поручения Кабинета Министров Республики Узбекистан, решения и распоряжения руководителей Узкомгосрезерв, заявления, жалобы, предложения граждан, а также другие документы, имеющие конкретные поручения и сроки их исполнения. Для данных документов автоматически должна ставиться отметка "На контроль", которая может быть снята при подготовке проекта резолюции или её утверждении.

Контролер осуществляет прием документа и формирует контрольные карточки по каждому контрольному пункту. Контрольная карточка информирует о сроках исполнения, о ходе выполнения и об отчете выполненного поручения. После согласования контролирующим лицом и утверждением руководителем отчета по поручению, документ снимается с контроля и направляется для регистрации как исходящий.

Контроль исполнения любого документа осуществляется на основании резолюции руководителя, контрольной карточки и задания. Для обеспечения контроля исполнения Система должна обеспечивать автоматизацию следующих функций:

- регистрация для каждого документа последовательного списка уточняющих резолюций при прохождении его по уровням иерархии управления с указанием сроков и исполнителей;
- ввод одного или нескольких исполнителей с указанием общего или персонального задания;
- снятие документов с контроля исполнения на основе утверждения отчетов исполнения;
- получение различных справок и отчетов по состоянию исполнительской дисциплины и возможно имеющимся нарушениям;
- разделение на контрольные пункты задач конкретных исполнителей с резолюции руководителя;
- отправка запроса на изменение резолюции руководителя со стороны контролера;
- включение подробных статистических данных и ситуационной панели по количеству задач в рабочем окне контролера.

4.2.3. Требования к поддержке процессов подготовки и согласования документов

Система должна поддерживать работу над проектами документов, включая:

- формирование проекта документа;
- возможность задания строгого маршрута движения проекта документа при его согласовании;
- прослеживание процесса согласования и визирования документов, предусматривая возможность их возврата на доработку;
- обеспечение процесса утверждения документа или возврата его на доработку.

4.2.4. Требования к возможностям настройки Системы

Система должна обеспечивать гибкие возможности настройки в соответствии с особенностями организационной структуры Заказчика и процессов работы с документами. В частности, обеспечивать возможности настройки:

- справочника видов документов, в том числе создания средствами администратора Системы новых видов документов и изменения реквизитов (их состава);

- прав пользователей Системы, в том числе возможность осуществлять ввод информации делопроизводственным персоналом вместо специалистов руководящего состава;

- обмена электронными документами;

- использования ЭЦП (включение и выключение этой функции);

- маршрутизации документов в зависимости от их типов и порядка обработки информации средствами администрирования Системы.

Для обеспечения функционирования территориально удаленных пользователей Система должна обеспечивать:

- возможность работы пользователя Системы в удаленном режиме;

- возможность интеграции со средствами организации коллективной работы над документами или наличие встроенных средств такой работы.

4.2.5. Требования к электронному документу в Системе

Система должна обеспечивать создание, а также работу с документами любых типов (приказы, распоряжения, поручения, инструкции, положения, уставы, письма, запросы, резолюции, справки, рапорты, схемы, договоры, акты, счета-фактуры, обращения (заявления, жалобы, предложения) и т. п.) в электронном виде.

Электронный документ в Системе должен представляться в виде регистрационно-контрольной карточки соответствующего входящего и исходящего документа, который содержит в себе реквизиты документа (регистрационный номер, вид документа и пр.), а также его содержание.

Ввод данных в регистрационно-контрольную карточку документа осуществляется как с клавиатуры, так и с использованием справочников Системы. Регистрационно-контрольная карточка документа может содержать ссылку на файлы документа, прикрепленные к ней.

4.2.6. Требования к справочникам Системы

В Системе должны быть использованы следующие общие справочники:

- подразделений

- должностей;

- сотрудников (пользователей Системы) каждого подразделения Узкомгосрезерв с их функциональными правами, уровнем доступа к документам различной степени конфиденциальности;

- видов документов;

- государственных органов и иных организаций, от которых поступает входящая и которым направляется исходящая корреспонденция;

- видов задач;

- видов доставки входящих документов;

- журналов регистрации.

4.2.7. Требования к схеме классификации, форматам и типам документов в Системе

Система должна поддерживать принятую в организации единую схему классификации документов и быть с ней совместимой.

Система должна предоставлять два механизма именования электронных папок в схеме классификации:

- механизм присваивания уникального структурированного цифрового или буквенно-цифрового кода каждой папке (делу);

- механизм задания текстового заголовка для каждой электронной папки (дела).

При создании новой папки (дела) Система обязательно должна автоматически включать в ее метаданные необходимые реквизиты.

Система обязательно должна позволять регистрировать документы установленных форматов и структур. Система должна предоставлять возможность расширять перечень поддерживаемых форматов по мере появления новых форматов.

Система должна поддерживать регистрацию офисных документов всех широко распространенных форматов. Система в обязательном порядке должна обеспечивать регистрацию следующих типов документов:

- сканированные бумажные документы;
- документы, созданные в офисных приложениях.

Система должна позволять регистрировать составные документы одним из следующих способов:

- как единый составной документ путем регистрации за одним номером;
- как набор связанных отдельных документов, путем регистрации за отдельным номером каждого документа, являющегося компонентом составного документа.

4.3. Требования к видам обеспечения

4.3.1. Требования к математическому обеспечению

Математические методы и алгоритмы, используемые для шифрования/дешифрования данных, а также программное обеспечение, реализующее их, должны быть сертифицированы уполномоченными организациями.

Математическое обеспечение Системы должно обеспечивать возможность эффективной разработки программных решений конкретных задач.

Математическое обеспечение Системы должно включать:

- типовые и разработанные методики и алгоритмы сбора и обработки информации (в том числе ввода данных в ПК, контроля достоверности данных и т.п.);
- алгоритмы поиска и сортировки данных.

Общие требования к математическому обеспечению:

- использование стандартной библиотеки классов;
- максимальное использование типовых методов и алгоритмов;
- используемые математические методы должны учитывать технические возможности технических и программных средств, иметь минимальные значения времени решения и занимаемой оперативной памяти;
- документация на математическое обеспечение (постановка задач и алгоритмы решения) должна обеспечивать однозначное толкование и возможность программирования без дополнительных разъяснений;
- допускается любая форма описания задач – формульная, табличная, блок- схема, UML диаграмма, словесное описание и др.

Алгоритмы математического обеспечения должны отвечать следующим требованиям:

- допускать декомпозицию на относительно простые блоки;
- максимально использовать возможности языков программирования в своем описании;
- обеспечивать функциональную взаимосвязь задач.

Алгоритмы поиска и сортировки данных, используемые при решении практически всех функциональных задач Системы, должны базироваться на процедурах в системном математическом обеспечении и используемых в СЭД. Эти алгоритмы должны обеспечивать поиск информации по заданным значениям признаков, формирования заданных структур информации и выполнение над ними необходимых операций. Алгоритмы формирования выходных документов должны быть максимально унифицированы, позволять при необходимости быстро изменять формы документов и использовать стандартные процедуры и программные средства.

Алгоритмы решения задач, при необходимости, могут включать методы оптимизации и эвристические процедуры для конкретных задач. Для задач большой размерности должны применяться декомпозиционные методы из решения, а при большой длительности решения задач необходимо предусмотреть контроль хода выполнения программ. Математические модели и методы их решения должны обеспечивать однозначность и единственность решения с заданной точностью (если специально не оговорено противоположное - несколько вариантов решения по выбору пользователя).

4.3.2. Требования к информационному обеспечению

Состав, структура и способы организации данных в системе должны быть определены на этапе технического проектирования. Уровень хранения данных в системе должен быть построен на основе современных реляционных или объектно-реляционных СУБД.

Средства СУБД, а также средства используемых операционных систем должны обеспечивать документирование и протоколирование обрабатываемой в системе информации. Структура базы данных должна поддерживать кодирование хранимой и обрабатываемой информации в соответствии с классификаторами (там, где они применимы).

Доступ к данным должен быть предоставлен только авторизованным пользователям с учетом их служебных полномочий, а также с учетом категории запрашиваемой информации.

Структура базы данных должна быть организована рациональным способом, исключающим единовременную полную выгрузку информации, содержащейся в базе данных ИС.

Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования.

В состав ИС должна входить специализированная подсистема резервного копирования и восстановления данных.

4.3.3. Требования к лингвистическому обеспечению

При реализации ИС должны применяться языки программирования высокого уровня.

При реализации ИС должен применяться язык взаимодействия пользователей и технических средств - «пользователь-интерфейс».

Кодирование и декодирование данных осуществляется в определенной стандартной форме.

Для реализации алгоритмов манипулирования данными необходимо использовать стандартный язык запроса к данным и его процедурное расширение.

Для описания предметной области (объекта автоматизации) должны использоваться средства автоматизации описания бизнес-процессов предметной области.

Для организации диалога ИС с пользователем должен применяться графический оконный пользовательский интерфейс. Интерфейс ИС должен быть мульти-язычным, по умолчанию использовать государственный язык (латиница).

4.3.4. Требования к программному обеспечению

Требования к системе управления базами данных (СУБД).

Сервер БД должен быть предназначен для хранения и обработки данных ИС.

В качестве ИС управления базами данных должна применяться реляционная СУБД, которая удовлетворяет следующим требованиям:

- поддерживает работу в архитектуре «клиент-сервер»;
- имеет встроенную ИС обработки транзакций;
- имеет средства распределенной обработки данных;
- поддерживает работу удаленных клиентов и передачу запросов и ответов на запросы по каналам связи.

Требования к средствам разработки прикладной логики. Сервер приложений должен производить основную обработку данных, обеспечивать связь с другими ИС, выполнять другие действия, составляющие бизнес-логику ИС. Сервер приложений должен взаимодействовать с сервером БД и клиентом.

Сервер приложений должен иметь набор специализированных средств в виде объектов и интерфейсов для организации взаимодействия с внешними ИС. Взаимодействие должно осуществляться посредством использования web-сервисов.

Требования к клиентской части. В качестве универсального средства визуализации информации в клиентской части предпочтительно использование web-интерфейса с поддержкой работы на всех основных версиях браузеров операционных систем для ПК и, по возможности, мобильных операционных систем.

4.3.5. Требования к техническому обеспечению

Техническое обеспечение ИС должно максимально и наиболее эффективным образом использовать существующие технические средства.

В состав комплекса должны быть следующие технические средства:

- Сервер БД;
- Сервер приложений;
- Сервер доступа;
- Рабочие станции для пользователей ИС;
- ПК администрирования.

Требования к программному обеспечению сервера приложений в локальной сети:

- Операционная система MS Windows Server 2019 или Linux (Ubuntu)
- Web-сервер IIS
- ASP.NET
- MS Office 2016 (и выше)

Требования к программному обеспечению сервера базы данных в локальной сети:

- Операционная система MS Windows Server 2019 или Linux (Ubuntu)
- СУБД Oracle

Программное обеспечение рабочей станции клиента в локальной сети:

- Операционная система Windows 10;
- Google Chrome 56.0 и выше
- MS Office 2016 (и выше);
- AdobeReader выше 2017 (для отображения pdf-файлов)

Характеристики сервера (минимум):

- Процессор Xeon E5-2699v3 или выше;
- ОЗУ не ниже 128 Gb;
- HDD: RAID 10 SAS/SSD 4 диска 4x 4Tb;
- Сетевая карта – 1 Gb/s и выше.

Характеристики рабочей станции клиента в локальной сети (минимум):

- процессор Intel Pentium 4 2.6 ГГц (и выше);
- ОЗУ 4 Гб (и выше);

Характеристики коммуникаций в корпоративной сети:

- подключение Сервера к сети по выделенному каналу со скоростью не менее 1 Гб/сек;
- клиентские рабочие станции должны быть подключены к сети со скоростью не менее 100 Мб/с.

4.3.6. Требования к организационному обеспечению

Состав сотрудников каждого из подразделений определяется штатным расписанием Заказчика, которое, в случае необходимости, может изменяться. Функции подразделений, участвующих в функционировании ИС или обеспечивающих эксплуатацию, устанавливаются Заказчиком.

К организации функционирования ИС и порядку взаимодействия персонала ИС и персонала объекта информатизации предъявляются следующие требования:

- в случае возникновения со стороны персонала необходимости изменения функциональности ИС, персоналом объекта информатизации должно быть описано дополнение ИС;

- проведении профилактических работ, все пользователи должны быть заранее (не менее чем за 3 дня) уведомлены (с указанием точного времени и продолжительности) о переходе ИС в профилактический режим.

К защите от ошибочных действий персонала ИС предъявляются следующие требования:

- должна быть предусмотрена ИС подтверждения правомерности пользователя при просмотре данных;

- для всех пользователей должна быть запрещена возможность удаления преднастроенных объектов и отчетности;

- для снижения ошибочных действий пользователей должно быть разработано полное и доступное руководство пользователя.

Для обеспечения правильной и безаварийной эксплуатации центрального узла Системы необходимо создание соответствующего подразделения или наём сторонней организации, обеспечивающих функционирование программных и аппаратных компонентов узла Системы.

Подразделение технического обеспечения должно обеспечивать бесперебойную работу серверов и клиентских рабочих станций Системы. Состав подразделения, в общем случае, должен включать следующие должности:

- администратор узла;
- инженеры по техническому обслуживанию узла;

Подразделение должно выполнять следующие функции:

- обеспечение бесперебойной работы серверов;
- обеспечение бесперебойной работы клиентских ПК;
- установка и настройка клиентского программного обеспечения;
- обеспечение бесперебойной работы сетевого оборудования и каналов связи;
- резервное копирование и, в случае необходимости, восстановление данных;
- защита информации от несанкционированного доступа.

4.3.7. Требования к методическому обеспечению

Нормативно-правовую базу ИС составляет действующее законодательство Республики Узбекистан. В случае изменения законодательных и нормативно-правовых актов или утверждения новых, разработка ИС и оформление документации по проекту должны учитывать эти изменения.

Перечень нормативной документации для использования при разработке ИС:

1) Закон Республики Узбекистан «Об электронном документообороте» от 29 апреля 2004 г., № 611-II;

Стандарты и руководящие документы:

1) O'z DSt 1047:2018. Информационные технологии. Термины и определения;

2) O'z DSt 1270:2009. Взаимодействие систем электронного документооборота.

Технические условия;

3) O'z DSt ISO/IEC/IEEE 12207:2018. MOD Информационные технологии. Процессы жизненного цикла программного обеспечения;

4) O'z DSt ISO/IEC TR 9294:2007. Информационные технологии. Руководство по управлению документированием программного обеспечения;

5) O'z DSt ISO/IEC 25051:2018. Разработка программного обеспечения. Разработка программного обеспечения. Требования к качеству и оценки систем программного продукта (SQuaRE). Требования к качества готового к использованию программного продукта (RUSP) и инструкции по тестированию.;

6) O'z DSt 1987:2018. Информационная технология. Техническое задание на создание информационной системы;

7) O'z DSt 1986:2018. Информационная технология. Информационные ИС. Стадии создания;

8) O'z DSt 1985:2018. Информационная технология. Виды, комплектность и обозначение документов при создании информационных систем;

9) O'z DSt 2590:2012. Информационная технология. Требования к интеграции и взаимодействию информационных систем государственных органов, используемых в рамках формирования Национальной информационной системы;

10) O'z DSt 2937:2015. Информационная технология. Обработка запросов при оказании интерактивных государственных услуг;

11) O'z DSt 2863:2014. Информационная технология. Интерактивные государственные услуги. Классификация и основные требования к формированию.

12) O'z DSt 2864:2014. Информационная технология. Межведомственная интеграционная платформа. Общие технические требования.

- 13) O‘z DSt 2295:2011. Электронный документ. Требования к формированию, применению и хранению.
- 14) O‘z DSt 1270:2009. Электронный документооборот. Взаимодействие систем электронного документооборота;
- 15) O‘zDSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
- 16) O‘zDSt 1106:2009 Информационная технология. Криптографическая защита информации. Функция хеширования.
- 17) O‘z DSt 1204:2009 Информационная технология. Криптографическая защита информации. Требования безопасности к криптографическим модулям.
- 18) O‘z DSt ISO/IEC 15408-1: 2016 Информационная технология. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель.
- 19) O‘z DSt ISO/IEC 15408-2: 2016 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
- 20) O‘z DSt ISO/IEC 15408-3: 2016 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
- 21) O‘z DSt ISO/IEC 27002: 2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
- 22) RH 45-215:2009 Руководящий документ. Положение об обеспечении информационной безопасности в сети передачи данных.
- 23) O‘z DSt ISO/IEC 27001:2016 Информационная технология. Методы обеспечения безопасности системы управления информационной безопасностью требования.
- 24) O‘zDSt 2814:2014 Информационная технология. Автоматизированные ИС. Классификация по уровню защищенности от несанкционированного доступа к информации;
- 25) O‘zDSt 2815:2014 Информационная технология. Межсетевые экраны. Классификация по уровню защищенности от несанкционированного доступа к информации;
- 26) O‘zDSt 2817:2014 Информационная технология. Средства вычислительной техники. Классификация по уровню защищенности от несанкционированного доступа к информации
- 27) O‘zDSt 1135:2007. Информационная технология. Требования к базам данных и обмену информацией между органами государственного управления и государственной власти на местах.
- 28) ИКН 17 2010 УзАСИ «Ведомственные строительные нормы. Проектирование структурированных кабельных систем и локальных вычислительных сетей».
- 29) RH 45-201:2011 «Технические требования к зданиям и сооружениям для установки средств вычислительной техники».
- 30) O‘z DSt 2875-2014 «Информационная безопасность. Требование к датацентрам. Инфраструктура и обеспечение информационной безопасности».
- 31) КМК 2.04.17-98 «Электрооборудование жилых и общественных зданий».
- 32) ГОСТ 12.1.030-81 (ИС стандартов безопасности труда. Электробезопасность. Защитное заземление, зануление) и правилами устройства электроустановок.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ ИС.

Номер этапа	Наименование этапов	Сроки выполнения		Исполнитель	Чем заканчивается этап
		начало	конец		
1	Разработка технического задания				Техническое задание
2	Разработка технического проекта				Технический проект
3	Разработка ИС				
4	Предварительные испытания				Отчет о тестировании
5	Разработка эксплуатационной документации Проведение обучения Проведение опытной эксплуатации				Отчет о проведении обучения Инструкция пользователя, администратора Акт ввода в опытную эксплуатацию
6	Ввод в промышленную эксплуатацию				Акт ввода в эксплуатацию
7	Сопровождение				Отчет о проведенных работах в режиме сопровождения

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ИС.

Контролю, испытаниям и приемке могут подвергаться как система в целом, так и ее отдельные очереди (пусковые комплексы), подсистемы и отдельные задачи.

Для Системы устанавливают следующие основные виды испытаний и приемки:

- Опытная эксплуатация;
- Промышленная эксплуатация.

При проведении испытаний Системы должно быть проверено и установлено соответствие Техническому заданию (ТЗ) на создание Системы следующего:

- качество выполнения комплексом программных и технических средств автоматизированных функций во всех режимах функционирования Системы;
- знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования Системы;
- полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования Системы;
- количественные и (или) качественные характеристики выполнения автоматических и автоматизированных функций Системы;
- другие свойства Системы, которым она должна соответствовать согласно требованиям Технического задания.

Испытания Системы проводятся на объекте Заказчика. По согласованию между Заказчиком и Поставщиком предварительные испытания и приемку программных средств

Системы допускается проводить на технических средствах Поставщика при создании условий получения достоверных результатов испытаний.

Статус и состав комиссии определяется Заказчиком.

По результатам испытаний составляются протоколы проведения с перечнем замечаний и акты завершения испытаний, на основании которых принимается решение о возможности (или невозможности) перехода к следующему виду испытания или приемки Системы в постоянную эксплуатацию. Виды испытаний могут повторяться до устранения всех замечаний к Системе и соответствующей корректировки эксплуатационной документации.

Испытания Системы выполняются после проведения отладки и тестирования поставляемых программных и технических средств Системы и представления Поставщиком соответствующих документов об их готовности к испытаниям, а также после ознакомления технических специалистов Заказчика с эксплуатационной документацией Системы.

Ввод Системы и отдельных ее частей в эксплуатацию представляет собой процесс постепенного перехода от существующих методов решения задач к автоматизированным методам.

В процессе опытной эксплуатации и испытаний проводится проверка готовности отдельных частей, комплексов и задач Системы, а также предъявленной документации к функционированию в реальных условиях. Эксплуатация Системы и ее частей начинается с момента утверждения акта приемки в эксплуатацию.

Возникшие в процессе предварительных испытаний и опытной эксплуатации дополнительные требования Заказчика, не предусмотренные в техническом задании, не являются основанием для отрицательной оценки результатов опытной эксплуатации и испытаний. Они могут быть удовлетворены по дополнительному соглашению в согласованные сроки.

6.1. Виды, состав, объем и методы испытаний системы и ее составных частей.

6.1.1. Предварительные испытания.

Предварительные испытания Системы проводятся для определения ее работоспособности и решения вопроса о возможности передачи Системы в опытную эксплуатацию.

Предварительные испытания проводятся на специально оборудованном стенде.

Предварительные испытания включают:

- автономные, для испытания отдельных модулей, задач и других частей Системы;
- комплексные, для испытания подсистем и Системы в целом, путем выполнения комплексных тестов.

При комплексных испытаниях допускается использовать в качестве исходной информации, данные, полученные при автономных испытаниях частей Системы.

6.1.2. Опытная эксплуатация.

Опытная эксплуатация Системы проводится для определения правильности принятых проектных решений и построенной информационной модели, для определения степени соответствия функциональности Системы требованиям пользователей и степени удобства работы с пользовательским графическим интерфейсом.

Работы по организации опытной эксплуатации включают:

- определение подразделений Заказчика, в которых будет проводиться опытная эксплуатация;
- определение ответственных лиц Заказчика за проведение опытной эксплуатации;
- определение сотрудников Заказчика участвующих в опытной эксплуатации;
- определение предварительных требований к бумажным формам учетно-отчетной документации и утверждение временного регламента ведения учета в организациях участвующих в опытной эксплуатации;
- развертывание Системы в выбранных подразделениях Заказчика;

- обучение сотрудников Заказчика правилам работы с Системой.

После начала опытной эксплуатации Системы ведется 15 дневная работа Системы сотрудниками Заказчика, которые во время опытной эксплуатации дают сведения об отказах, сбоях, аварийных ситуациях. При их наличии сведения фиксируются и передаются Исполнителю.

Информация, вводимая в Систему на этапе опытной эксплуатации, должна быть удалена из хранилища данных при переходе к этапу промышленной эксплуатации и не может быть использована для формирования каких бы то ни было официальных отчетных форм.

Сдача в промышленную эксплуатацию производится после окончания опытной эксплуатации.

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ИС К ВВОДУ В ДЕЙСТВИЕ.

При подготовке ИС к вводу в действие необходимо выполнить перечень мероприятий:

1) Технические мероприятия

- осуществлена подготовка помещения для размещения программного-аппаратного комплекса ИС в соответствии с требованиями, приведенными в настоящем техническом задании;

- осуществлена закупка и установка необходимого программного-аппаратного комплекса;

- организовано необходимое сетевое взаимодействие.

2) Организационные мероприятия

Силами Заказчика должны быть решены организационные вопросы по взаимодействию с ИС-источниками данных. К данным организационным вопросам относятся:

- организация доступа к базам данных источников;

- определение регламента информирования об изменениях структур систем-источников;

- выделение ответственных специалистов со стороны Заказчика для взаимодействия с проектной командой по вопросам взаимодействия с ИС-источниками данных;

- обучение пользователей ИС.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ.

При разработке проектной, рабочей и эксплуатационной документации Исполнитель должен руководствоваться государственным стандартом O'zDSt 1985:2018 Информационные технологии. Виды, комплектность и обозначение документов при создании информационных систем.

Руководитель организации
разработчика ТЗ

ФИО

Непосредственный руководитель
исполнителя

ФИО

Исполнитель

ФИО