

Техническое задание на услугу по оказанию технической поддержки системы электронного документооборота на базе программного обеспечения Landocs.

1.1 Основные понятия технической поддержки

Техническая поддержка организуется на основе инцидентной модели. Каждое событие, связанное с обращением за технической поддержкой (далее - Заявкой), считается инцидентом, а все действия, связанные с ним – обработкой инцидента.

Для классификации инцидентов при регистрации Заявки применяется классификационный параметр – «Критичность инцидента».

Критичность инцидента может принимать значения:

- Высокая;
- Средняя;
- Низкая.

Уровень критичности первоначально присваиваются инциденту при регистрации Заявки, но в дальнейшем, при обработке инцидента, может быть изменен.

Критерии присвоения инциденту уровня критичности приведены в Приложении А настоящего Порядка.

Информация о выявленных ошибках регистрируется в Журнале учёта инцидентов с соответствующей пометкой в графе «Вид обращения». Форма Журнала учета инцидентов приведена в приложении Б.

1.2 Объект технической поддержки

Объектом технической поддержки является Система.

Потребителями технической поддержки являются:

- Администраторы Системы – в части круга вопросов, касающихся настройки и обслуживания Системы;
- Пользователи Системы – в части вопросов, касающихся функционирования Системы.

1.3 Взаимодействие сторон в рамках технической поддержки

Исполнитель при заключении договора предоставляет следующие каналы обращения за технической поддержкой:

- Телефон технической поддержки:
- Адрес электронной почты:
- Адрес сайта для формирования и/или отслеживания состояния Заявок.

Заказчик при заключении договора предоставляет следующие сведения:

- ФИО, должность, e-mail и телефоны ответственного специалиста Заказчика, отвечающего за взаимодействие с Исполнителем по вопросам технической поддержки.

Ответственный специалист со стороны Заказчика, осуществляет:

- Сбор обращений по проблемам работы с Системой от инициаторов обращений – сотрудников Заказчика, работающих с Системой;
- Предварительное определение соответствия каждого обращения составу вопросов, решаемых в рамках технической поддержки;
- Формулирование Заявки на техническую поддержку в соответствии с требованиями к Заявке (Приложение В);
- Направление Заявки на техническую поддержку Исполнителю;
- Предоставление дополнительной информации по Запросу от Исполнителя;
- Обеспечение возможности удаленного доступа Исполнителя к рабочему месту или серверу Заказчика по запросу Исполнителя;
- Контроль исполнения Заявки со стороны Заказчика, направление претензий по качеству выполнения Заявок;
- Отслеживание хода исполнения Заявки и/или устранения недостатков в ее исполнении;
- Получение от Исполнителя и фиксация отчета об исполнении Заявки.

Исполнитель, получив Заявку по одному из указанных каналов, регистрирует Заявку в Системе учета заявок и сообщает ответственному специалисту номер заявки по указанному адресу электронной почты ответственного специалиста со стороны Заказчика.

Исполнитель, в процессе исполнения Заявки обращается за дополнительной информацией к ответственному специалисту со стороны Заказчика и сотруднику Заказчика – инициатору обращения.

1.4 Ограничения технической поддержки

Техническая поддержка **оказывается** в следующих случаях:

- Требуется консультация:
 - o Пользователю – по вопросам, связанным с использованием Системы¹;
 - o Администратору – по особенностям настройки и обслуживания Системы (включая настройку электронной подписи в Системе);
- Возникла нештатная ситуация в работе Системы, требующая помощи в устранении проблемы:
 - o Клиентская часть Системы не запускается при включении или перезагрузке компьютера, на котором она установлена;
 - o При включении или в процессе работы клиентской части Системы возникают ошибки, сопровождаемые сообщениями об ошибке;
 - o В работе клиентской части происходят сбои в процессе работы, выражающиеся в зависании (отсутствии отклика в течение более чем 3-х минут, за исключением времени формирования отчета) или самопроизвольном выключении клиентского приложения LanDocs;
 - o Серверная часть Системы не запускается при включении или перезагрузке сервера;
 - o При включении, перезагрузке или в процессе работы серверной части Системы возникают ошибки, сопровождаемые сообщениями об ошибке;
 - o В работе серверной части (серверные компоненты LanDocs или СУБД в составе Системы) систематически возникают сбои;
 - o В других случаях, когда серверная или клиентская часть системы не устанавливается, не настраивается или не функционирует должным образом.

Техническая поддержка **не оказывается** в следующих случаях и по следующим основаниям:

¹ Оказание консультации не отменяет необходимости пользователю пройти предусмотренное обучение по работе с системой и изучить Руководство пользователя. Консультация оказывается только по вопросам, ответ на которые пользователь не может найти в документации.

- Обращение по вопросам, не относящимся напрямую к функциям, техническим особенностям, специфике эксплуатации или обслуживанию Системы;
- Обращение по вопросам использования Системы, рассмотренным в документации;
- Обращение по вопросам, выходящим за рамки документированного функционала Системы (в том числе и административного);
- Обращения, связанные с диагностика, обслуживанием и ремонтом любого аппаратного и программного обеспечения, за исключением настройки и обновления Системы;
- Доработка и настройка Системы в части расширения или изменения функциональности системы (включая приём и регистрацию заявок или пожеланий на подобную доработку);
- Устранение проблем нештатного функционирования Системы, вызванных несоответствием программных и аппаратных средств Системы техническим требованиям к Системе.

1.5 Способы осуществления технической поддержки

Диагностирование проблемы по заявке пользователя осуществляется:

- На основании предоставленных пользователем описания проблемы и снимков экрана, демонстрирующих проявление проблемы;
- По результатам ознакомления с проявлением проблемы и действиями пользователя, приведшими к проблеме, с применением средств удаленного доступа (TeamViewer) к рабочему месту пользователя или серверу.

Консультирование по разрешению проблемы осуществляется:

- Путём предоставления устных рекомендаций (по телефону);
- Путём предоставления письменных рекомендаций (по электронной почте);
- Путем демонстрации необходимого порядка действий по устранению или предотвращению проблемы с применением средств удаленного доступа (TeamViewer).

В рамках технической поддержки оказывается только дистанционная консультативная поддержка пользователей и администраторов Заказчика с привлечением технических специалистов Исполнителя. Выезд представителей Исполнителя на объекты Заказчика не предусмотрен.

2 Порядок осуществления технической поддержки

Техническая поддержка оказывается в соответствии со следующим порядком:

- В случае возникновения потребности в технической поддержке, сотрудник Заказчика обращается с описанием проблемы к ответственному сотруднику Заказчика.
- Ответственный сотрудник Заказчика по возможности самостоятельно устраняет проблему или формирует Заявку по технической поддержке, если проблема относится к вопросам технической поддержки и направляет Заявку по одному из указанных в п. 1.3 каналов обращения.
- Исполнитель:
 - О получает и регистрирует Заявку в системе учета Заявок, сообщает на адрес электронной почты ответственного сотрудника Заказчика идентификатор Заявки;
 - О диагностирует проблему, при необходимости привлекая технических специалистов Исполнителя, запрашивая дополнительную информацию у Заказчика, используя средства удаленного доступа;
 - О в случае, если Заявка не относится к сфере технической поддержки, а соответствующая проблема может быть решена исключительно доработкой Системы, Исполнитель закрывает Заявку, сообщая основание закрытия и фиксируя постановку на доработку Системы для обеспечения ее реализации в рамках возможного договора на развитие Системы;
 - О в случае, если Заявка не может быть решена в рамках технической поддержки, Исполнитель закрывает Заявку, сообщая основание закрытия и, возможно, рекомендации по альтернативным способам решения проблемы ответственному сотруднику Заказчика;

- присваивает Заявке уровень критичности и приоритет; определяет плановый срок исполнения Заявки;
 - сообщает ответственному сотруднику Заказчика плановый срок исполнения Заявки;
 - исполняет Заявку, взаимодействия с инициатором Заявки и ответственным сотрудником Заказчика;
 - сдает результаты исполнения Заявки ответственному сотруднику Заказчика, направляя уведомление об исполнении Заявки с кратким описанием проведенных мероприятий на адрес электронной почты ответственного сотрудника Заказчика.
- Ответственный сотрудник Заказчика принимает результаты исполнения Заявки или сообщает замечания Исполнителю.
 - Исполнитель при необходимости устраняет замечания и повторно сдает результаты ответственному сотруднику Заказчика.
 - Если результаты исполнения приняты (отсутствуют замечания в течение 3-х дней с момента сдачи результатов исполнения Заявки), Заявка считается исполненной и закрывается.

Все этапы работы с Заявкой фиксируются в журнале учета Заявок.

В любой момент ответственный сотрудник Заказчика может получить информацию о ходе исполнения Заявки через систему учета заявок, указав идентификатор Заявки или обратиться с вопросами относительно ее исполнения по телефону или электронной почте Исполнителя.

Ответственный сотрудник Заказчика может в любой момент отозвать незакрытую Заявку, если проблема решена без участия специалистов техподдержки, либо потеряла свою актуальность через систему учета заявок или обратившись по электронной почте, указав идентификатор Заявки и основание для ее отзыва.

Исполнение Заявки может быть отложено или даже невозможно по следующим основным причинам:

- Невозможно повторно воспроизвести проблему на рабочем месте или сервере Заказчика;
- Заказчик не может предоставить достаточно исходной информации для выявления и решения проблемы.

- Исполнение Заявки требует доработки функционала и/или выпуска обновления для программного продукта;
- Заявка сформулирована некорректно, дополнительная информация предоставляется в недостаточном объеме и/или несвоевременно.

3 Обязанности Исполнителя и Заказчика

3.1 Исполнитель обязан:

Для оказания технической поддержки Исполнитель обязан обеспечить прием и регистрацию Заявок Заказчика на техническую поддержку по указанным в п. 1.3 каналам обращений.

В процессе оказания технической поддержки Исполнитель должен осуществлять в рамках ограничений п. 1.4:

- оперативное восстановление работоспособности Системы в случае сбоев;
- консультирование по вопросам администрирования Системы;
- анализ и исправление ошибок пользователей и администраторов Системы, возникающих при работе с Системой;
- поддержку пользователей и консультации по использованию Системы;
- проведение анализа нетиповых ситуаций, выработку решений по устранению возникших проблем;
- настройку конфигураций, не затрагивающих основные алгоритмы Системы;
- восстановление баз данных в случае их повреждения;
- передача обновлений Системы, обновление инструкций.

При предоставлении Акта сдачи-приемки услуг Исполнитель должен представить Заказчику заполненный Журнал учёта инцидентов за отчетный период.

3.2 Заказчик обязан

Для получения технической поддержки Заказчик должен обеспечить необходимый уровень квалификации пользователей и администраторов Системы в части вопросов работы с Системой. В частности, Заказчик должен провести подготовку пользователей и администраторов в соответствии с программами подготовки, разработанными Исполнителем, обеспечить явку сотрудников на проводимые Исполнителем мероприятия по подготовке пользователей и администраторов, а также обеспечить ознакомление пользователей и администраторов с эксплуатационной документацией на Систему

(Руководство пользователя, Руководство администратора) и иными информационными материалами, предоставленными Исполнителем.

В период действия технической поддержки Заказчик должен:

1. Обеспечивать доступ к работе с Системой только сотрудников, прошедших необходимый инструктаж и ознакомленных с эксплуатационной документацией на Систему – руководствами пользователей (для пользователей) и руководствами администраторов (для администраторов), входящими в комплект документации на Систему;
2. Эксплуатировать Систему исключительно в соответствии с эксплуатационной документацией на неё, в т.ч.:
 - а) Выполнять все предусмотренные эксплуатационной документацией действия и мероприятия по обслуживанию Системы (периодическое резервное копирование данных, диагностирование работоспособности Системы и её компонентов);
 - б) Соблюдать все требования, предусмотренные соответствующей эксплуатационно-технической документацией на техническую инфраструктуру, на которой развёрнута и эксплуатируется Система (КТС, системное и общее ПО, оборудование передачи данных, системы электроснабжения, вентиляции и кондиционирования и т.п.) и выполнять регламентные мероприятия по обслуживанию инфраструктуры;
3. Обеспечивать и поддерживать своими силами работоспособность КТС, на котором развёрнута Система;
4. Обеспечивать (в случае необходимой замены компонентов КТС или при установке обновлений общего и системного ПО) выполнение требований, предъявляемых к КТС в части состава и технических характеристик КТС, общего и системного ПО согласно приложению Г;
5. Не допускать самостоятельного (без согласования с Исполнителем) изменения конфигурации Системы или её компонентов, в частности:
 - а) Изменения состава и технических характеристик КТС, использованных для развертывания Системы (как серверной, так и клиентской частей);
 - б) Изменения состава и технических характеристик общего и системного ПО;
 - в) Установки обновлений общего и системного ПО (операционной системы, СУБД);
 - г) Установки на сервера и клиентские рабочие места дополнительного ПО (антивирусы, файрволы и т.п.), влияющего на работу Системы или её

компонентов (в т.ч. путём блокировки портов, запрета выполнения приложений и т.п.);

д) Изменения выполненных при разворачивании Системы настроек соединения серверной части с СУБД;

е) Изменения настроек фаерволов и иных системных или сервисных приложений и служб в части блокировки портов, разрешения/запрета протоколов и т.п., используемых Системой;

6. Обеспечить наличие на всех серверах и компьютерах, на которых установлено и эксплуатируется ПО Системы, специального ПО удалённого доступа TeamViewer.

Перечень принятых сокращений

Полное наименование	Сокращение
Комплекс технических средств	КТС
Программное обеспечение	ПО
Федеральная служба по ветеринарному и фитосанитарному контролю	РСХН, Россельхознадзор
Система электронного документооборота	СЭД, Система
Техническая поддержка	ТП, Техподдержка

Перечень принятых терминов

Термин	Определение
Базовая программная платформа	Программная платформа LanDocs, на которой построена система электронного документооборота (СЭД)
Дистанционный (удалённый) доступ	Подключение к удалённому компьютеру/серверу с помощью специального программного обеспечения, позволяющего выполнять действия по управлению удалённым компьютером дистанционно
Заказчик	Центральный аппарат Федеральной службы по ветеринарному и фитосанитарному контролю (Россельхознадзор)
Инцидент	Любое событие, приводящее к нарушению нормального функционирования системы электронного документооборота, либо оказывающее или способное оказать влияние на её нормальное функционирование
Исполнитель	
Консультация	Ответ на устный или письменный запрос Заказчика о действиях, которые необходимо выполнить для получения нужного результата
Критичность инцидента	Степень важности проблемы, вызвавшей инцидент

Термин	Определение
Обращение	Обращение представителя Заказчика за услугами технической поддержки
Объект эксплуатации	Центральный аппарат Россельхознадзора, в котором эксплуатируется Система
Ошибка персонала	Неверные действия, не предусмотренные эксплуатационной документацией на Систему (Руководством пользователя и Руководством администратора) в части работы с Системой или её обслуживания
Приоритет инцидента	Свойство инцидента, определяющее очередность его обработки в потоке заявок
Проблема	Сложный вопрос или задача, требующая решения
Техническая поддержка	Совокупность мероприятий по технической поддержке системы электронного документооборота центрального аппарата Федеральной службы по ветеринарному и фитосанитарному контролю, выполняемых Исполнителем в соответствии с Договором о технической поддержке

Критерии оценки уровня критичности обращений

Выделяются три уровня критичности:

- Высокий – проблема связана с невозможностью выполнения обязательных операций в Системе;
- Средний – проблема связана с затруднениями выполнения операций в Системе;
- Низкий – проблема не связана с сокращением доступной функциональности Системы.

Высокий уровень критичности присваивается:

- При сбоях Системы, требующих консультаций по её восстановлению;
- При нетиповых ситуациях, в которых невозможно функционирование серверной части Системы на объекте эксплуатации;
- При невозможности пользователем с ролями «Руководитель» или «Помощник руководителя» выполнить штатные действия, предусмотренные задокументированным функционалом Системы.

Средний уровень критичности присваивается:

- При заметном снижении производительности в процессе эксплуатации Системы (большое время реакции Системы на событие, инициированное пользователем в интерфейсе рабочего места);
- При нетиповых ситуациях, в которых возможно функционирование серверной части Системы на объекте эксплуатации, но возникают затруднения с нормальным использованием задокументированных функций Системы на клиентских рабочих местах;

Низкий уровень критичности присваивается:

- При всех проблемах, не связанных с работоспособностью Системы и корректностью её работы.

В случае невозможности однозначно установить уровень критичности для поступившей заявки на поддержку, по умолчанию присваивается средний уровень критичности.

Для сообщений об ошибках Системы устанавливается высокий уровень критичности.

Принятую и зарегистрированную заявку Исполнитель должен обработать в установленные сроки.

Приоритет Заявки устанавливается в зависимости от присвоенного при регистрации уровня критичности инцидента согласно таблице 1:

Таблица 1 - Соответствие уровня критичности и приоритета Заявки

Уровень критичности	Приоритет
Высокий	1
Средний	2
Низкий	3

В процессе обработки Заявки приоритет может быть изменен специалистами Исполнителя в зависимости от выявленных обстоятельств:

- Для инцидентов с уровнем критичности «Средний» приоритет Заявки может быть поднят до «1» либо снижен до «3»;
- Для инцидентов с уровнем критичности «Низкий» приоритет Заявки может быть повышен до «2»;
- Приоритет инцидентов с уровнем критичности «Высокий» изменён быть не может.

Плановый срок исполнения Заявки устанавливаются в соответствии с приоритетами согласно таблице 2:

Таблица 2 – Плановый срок исполнения Заявки в зависимости от приоритета

Приоритет	Срок
1	Один рабочий день с даты регистрации Заявки
2	Два рабочих дня с даты регистрации Заявки
3	Три рабочих дня с даты регистрации Заявки

Форма Журнала учета инцидентов

№ п/п	Дата и время регистрации инцидента	Вид обращения	Ф.И.О. Должность	Подразделение	Контактные данные Телефон, E-mail	Критичность инцидента	Описание инцидента	Плановый срок разрешения инцидента	Дата закрытия инцидента	Описание решения	Дополнительная информация

Состав Заявки на техническую поддержку

- ФИО обратившегося сотрудника (по умолчанию – ответственный сотрудник Заказчика);
- Контактные данные (по умолчанию – контактные данные ответственного сотрудника Заказчика);
- Контактные данные сотрудника Заказчика – инициатора обращения:
 - o e-mail
 - o телефон
 - o Зарегистрированное у Исполнителя имя рабочего места или сервера (или идентификатор/пароль при отсутствии регистрации) в TeamViewer, на котором обнаружена проблема.
- Вид обращения («Вопрос» или «Ошибка»);
- Описание проблемы

При описания ошибки следует указать:

- Внешнее проявление;
- Частота возникновения проблемы (единоразово, периодически, постоянно);
- Перечень действий, приводящих к возникновению проблемы;
- Систематичность проявления проблемы (один раз, иногда, постоянно);
- Снимки экрана («скрин-шоты») с внешним проявлением проблемы.

По запросу Исполнителя предоставляются:

- дополнительная информация по проблеме;
- дополнительные снимки экрана («скрин-шоты») с внешним проявлением проблемы;
- демонстрация порядка действий, приводящих к возникновению проблемы, с применением средств удаленного доступа (TeamViewer).

Технические требования к Системе

1 Общие требования к аппаратно-программному обеспечению Системы

Для нормальной работы Системы необходимо, чтобы аппаратные средства, на которых развёрнуты серверные компоненты, СУБД и клиентские рабочие места, а также системное и служебное программное обеспечение, установленное на этих аппаратных средствах, по номенклатуре и своим техническим характеристикам соответствовали нижеприведённым требованиям. В случае несоответствия фактической номенклатуры и характеристик аппаратно-программных средств приведённым ниже требованиям, нормальная устойчивая работа системы не гарантируется.

2 Требования к архитектуре

Сетевая инфраструктура Системы должна соответствовать схеме, представленной на рисунке 1:

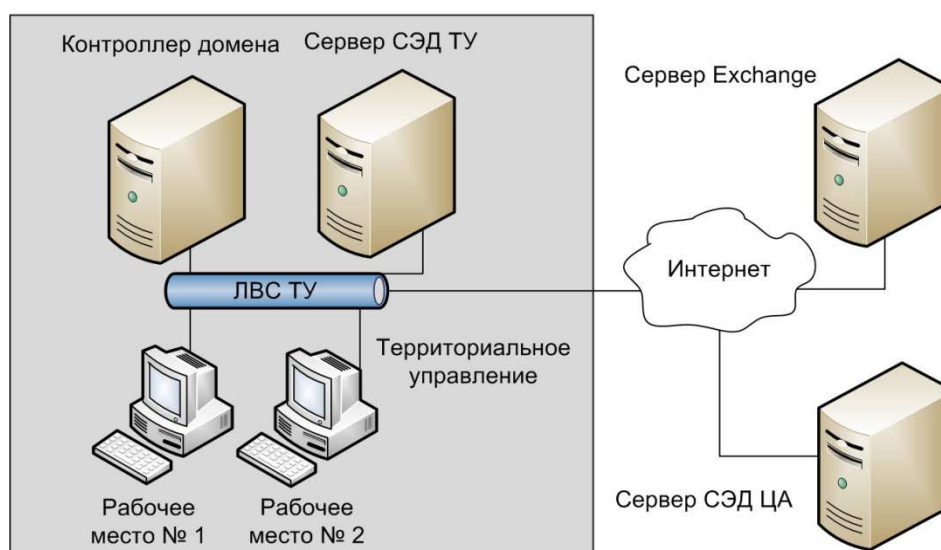


Рисунок 1 - Схема сетевой инфраструктуры

Для инфраструктуры должны выполняться следующие требования:

- Серверная часть Системы (серверные компоненты LanDocs и СУБД в составе Системы) должна устанавливаться на выделенные сервера;
- Не допускается использование СУБД, входящей в состав СЭД РСХН, для сторонних систем;
- Рабочие места и сервер ЦА должны быть в одном домене.
- Рабочие места и сервер ЦА должны иметь открытыми порты 80 и 443 (для исходящих соединений) или (альтернативно) должен быть открыт только порт 5938.

3 Требования к аппаратному обеспечению Системы

Аппаратные средства, используемые для разворачивания Системы, должны иметь следующие технические характеристики.

Серверы СУБД и LanDocs:

- Процессор:
 - o Количество, не менее – 2;
 - o Количество ядер, не менее – 4;
 - o Тип – Intel Xeon;
- Оперативная память:
 - o Объем, не менее – 48 ГБ;
 - o Тип, не ниже – DIMM DDR3;
 - o Рабочая частота, не ниже – 1066/1333 МГц;
- Жёсткий диск:
 - o Количество, не менее – 3;
 - o Ёмкость, не менее – 450 ГБ (каждый);
- Сетевые карты:
 - o Тип – Ethernet;
 - o Скорость, не менее – 1000 Мбит/с.

Компьютер для клиентского рабочего места:

- Процессор:
 - o Тип (не хуже) – Intel Pentium G620 ,
 - o Частота (не ниже) – 2600 МГц;
- Оперативная память:
 - o Объём, не менее – 2 ГБ;
- Жёсткий диск:
 - o Ёмкость, не менее – 250 ГБ;
- Сетевые карты:
 - o Пропускная способность – 10 Мбит/с.

4 Требования к программному обеспечению СИСТЕМЫ

Программные средства, используемые для поддержания Системы, должны иметь следующие номенклатуру и характеристики:

Серверная часть:

- Операционная система – Windows Server 2008 R2 Enterprise 64x или Windows Server 2012 R2 Enterprise 64x;
- СКЗИ – Крипто-Про 3.6;
- СУБД – Microsoft SQL Server-2008 R2;
- Средство удаленного доступа TeamViewer (в режиме Host);
- Серверные компоненты LanDocs:
 - o LanDocs: Делопроизводство;

- o LanDocs: Сервер документов;
- o LanDocs: Подсистема безопасности;
- o LanDocs: Подсистема XML-обмена.

Клиентская часть:

- Операционная система – Windows XP, Windows Vista, Windows 7²;
- СКЗИ – Крипто-Про 3.6;
- Клиентская часть Landocs:
 - o LanDocs: Делопроизводство;
 - o LanDocs: Подсистема безопасности.

Не допускается применение ПО других производителей для вышеуказанных целей.

Работа Системы с ПО гарантируется при соблюдении перечисленных версий программных продуктов. Работа на иных версиях ПО не гарантируется.

5 Требования к способам и средствам обеспечения информационной безопасности

5.1 Требования к удостоверяющему центру

С целью обеспечения административной и технической поддержки использования ЭП, Удостоверяющий центр должен:

- соответствовать требованиям, установленным приказом Министерства связи и массовых коммуникаций Российской Федерации от 23.03.2009 № 41
- иметь возможность осуществлять свои обязательства через свои обособленные подразделения (представительства, филиалы, обособленные рабочие места) или уполномоченных представителей (агентов и т.д.)

Кроме того, к УЦ предъявляются следующие дополнительные требования:

- Автоматизированная система удостоверяющего центра должна соответствовать требованиям нормативной документации по безопасности конфиденциальной информации для класса защищенности от несанкционированного доступа не ниже 1Г.
- УЦ должен иметь действующие лицензии, выданные уполномоченным федеральным органом исполнительной власти в соответствии с федеральным Законом №99 от 4 мая 2011 г. «О лицензировании отдельных видов деятельности»:

- o на распространение шифровальных (криптографических) средств;

² Поддерживаются все подверсии указанных операционных систем. Более ранние ОС не поддерживаются. Работа с более поздними ОС не проверялась и не гарантируется.

- о на техническое обслуживание шифровальных (криптографических) средств;
 - о на предоставление услуг в области шифрования информации.
- Либо, в качестве альтернативы предыдущему пункту, УЦ должен иметь действующие лицензии со следующими пунктами Приложения к Положению о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденному Постановлением Правительства РФ № 313 от 16 апреля 2012 г.:
- о 12 «Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств»;
 - о 13 «Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем»;
 - о 15 «Монтаж, установка (инсталляция), наладка средств изготовления ключевых документов»;
 - о 21 «Передача шифровальных (криптографических) средств»;
 - о 25 «Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей»;
 - о 28 «Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых

документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств».

- Средства криптографической защиты информации, используемые УЦ, должны быть сертифицированы и эксплуатироваться в полном соответствии с требованиями эксплуатационной и нормативной документации;
- Сопровождение выпущенных сертификатов должно обеспечиваться в течение срока действия ЭЦП и включать внеплановую замену СКП по заявкам пользователей в течение одного рабочего дня, и техническую (консультационную) поддержку конечных пользователей со стороны Заказчика, в течение срока действия ЭП. ЭП выдается сроком не менее чем на 1 год.
- В случае получения заявки о необходимости прекращения действия сертификата ЭП УЦ должен внести информацию о прекращении действия этого сертификата в реестр квалифицированных сертификатов в течение 1 рабочего дня с момента получения заявления. Действие сертификата прекращается с момента внесения записи об этом в реестр квалифицированных сертификатов.
- УЦ должен обеспечивать выполнение целевых функций, связанных с оказанием услуг, круглосуточно в течение всего срока действия, используя необходимые организационно-технические мероприятия, а также обеспечивать восстановление работоспособности в течение времени, не превышающего 1 (одного) часа после фиксации УЦ отказа.
- УЦ должен обеспечить круглосуточную техническую (контактную) поддержку конечным пользователям со стороны Заказчика контактным центром, обладающим общефедеральным бесплатным контактным номером телефона.
- УЦ должен быть аккредитован в соответствии с требованиями Закона 63-ФЗ «Об электронной подписи» и в соответствии с требованиями Приказа Министерства связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) от 23 ноября 2011 г. N 320 г.

В части функциональности к УЦ предъявляются следующие требования:

- УЦ использует сертифицированные средства криптографической защиты информации (средства электронной подписи);

- УЦ обеспечивает изготовление СКП, допущенных к использованию в процессе взаимодействия со всеми государственными и муниципальными органами власти, с которыми Россельхознадзором организовано взаимодействие в электронном виде.
- УЦ использует криптографические алгоритмы ГОСТ Р 34.11/34.10-2001 для формирования электронной подписи (ЭП) в инфраструктуре открытых ключей;
- УЦ обеспечивает временное приостановление действия СКП; возобновление действия СКП; аннулирование (отзыв) СКП; формирование и распространение списков аннулированных (отозванных) и приостановленных СКП в течение одного рабочего дня с момента получения заявки. Списки отозванных СКП должны предоставляться ежедневно без перерыва (включая выходные и праздничные дни) в режиме 24 часов;
- УЦ создает ключи электронных подписей по обращению Заказчика с гарантией сохранения в тайне закрытого ключа электронной подписи;
- УЦ ведет реестр сертификатов ключей подписей, обеспечивает его актуальность и возможность свободного доступа к нему участников информационных систем;
- УЦ проверяет уникальность открытых ключей электронных подписей в реестре сертификатов ключей подписей и архиве удостоверяющего центра;
- УЦ выдает сертификаты ключей подписей в форме документов на бумажных носителях и (или) в форме электронных документов с информацией об их действии;
- УЦ осуществляет по обращениям пользователей сертификатов ключей подписей подтверждение подлинности электронной цифровой подписи в электронном документе в отношении выданных им сертификатов ключей подписей.
- УЦ должен предоставлять сертификаты и СОС в виде файлов в одной из следующих кодировок: DER, Base64, PEM.

5.2 Требования к средствам криптографической защиты информации

Средства криптографической защиты информации должны быть совместимы с программным обеспечением, установленным на компьютерах используемых конечными пользователями со стороны Заказчика и поддерживать следующие платформы:

- Windows XP (x86, x64);
- Windows 2003 (x86, x64, IA64);
- Windows Vista (x86, x64);
- Windows Server 2008 (x86, x64, IA64);
- Windows 7 (x86, x64).

Для выполнения криптографических преобразований должны использоваться алгоритмы, устанавливаемые государственными стандартами Российской Федерации:

- Алгоритм формирования и проверки ЭЦП, реализованный в соответствии с требованиями ГОСТ Р 34.10-2001 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».
- Алгоритм выработки значения хэш-функции должен соответствовать требованиям ГОСТ Р 34.11-94 «Информационная технология. Криптографическая защита информации. Функция хэширования».
- Алгоритм зашифровывания/расшифровки данных и вычисления имитовставки должен быть реализован в соответствии с требованиями ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

5.3 Требования к носителям ключевой информации

В качестве носителя ключевой информации для пользователя должны использоваться сертифицированные электронных идентификаторов Rutoken/eToken, и соответствовать следующим требованиям:

- Быть изготовленным в форм-факторе usb-ключа;

- Иметь оценочный уровень доверия ОУД=2 в соответствии с руководящим документом «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Госкомкомиссия России, 2002);
- Соответствовать требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999) - по 4 уровню контроля и может использоваться при создании автоматизированных систем до класса защищенности 1Г включительно и при создании информационных систем персональных данных до 1 класса включительно;
- Объем защищенной памяти носителя должен быть не менее-72 кб на микросхеме смарт-карты.

Носители ключевой информации и электронные идентификационные элементы должны обеспечивать:

- устойчивость к воздействию отказов и сбоев, в том числе инициированных внешними воздействиями (облучениями);
- эргономические и технические характеристики, пригодные для массового использования.

Пользователям должно быть запрещено делать неучтенные копии ключевой информации содержащейся в ключевых носителях.

5.4 Требования к сертификатам и спискам отозванных сертификатов для функционирования LanDocs

Сертификаты и списки отозванных сертификатов (далее – СОС), должны выпускаться в соответствии с международным стандартом серии Public Key Infrastructure (X.509).

Основные поля сертификата должны соответствовать перечню полей согласно Стандарту X. 509:

- Version – версия формата сертификата (опционально);
- SerialNumber – серийный номер сертификата;

- Signature – алгоритм подписи сертификата;
- Issuer – издатель сертификата;
- Validity – срок действия сертификата;
- Subject – владелец сертификата;
- SubjectPublicKeyInfo – открытый ключ;
- IssuerUniqueID – идентификатор издателя (опционально);
- SubjectUniqueID – идентификатор пользователя (опционально);
- Extensions – расширения сертификата.

К основным полям сертификата предъявляются следующие требования:

- Поле «Version» должно содержать значение 2 (соответствует версии 3);
- Поле «Subject» должно содержать DN владельца сертификата;
- Поля «IssuerUniqueID» и «SubjectUniqueID» – не должны использоваться. Кроме того, в сертификате должны присутствовать следующие расширения:
 - Key Usage (OID = 2.5.29.15);
 - Назначение использования ключей. Должно включать значения digitalSignature/nonRepudiation для ключей подписи и keyEncipherment для ключей шифрования;
 - Subject Key Identifier (OID = 2.5.29.14);
- Идентификатор ключа владельца сертификата.

Все сертификаты, выпущенные УЦ, должны иметь различные значения этого поля. Для большинства УЦ это означает, что выпуск более одного сертификата на один открытый ключ пользователя является недопустимым.

- Authority Key Identifier (OID = 2.5.29.35)
- Идентификатор ключа издателя в форме keyIdentifier. Может отсутствовать только в самоподписанных сертификатах.

Для физического лица должен быть указан страховой номер индивидуального лицевого счета гражданина (СНИЛС) в системе обязательного пенсионного страхования (OID = 1.2.643.100.3).

Для юридического лица должны быть указаны:

- основной государственный регистрационный номер (далее – ОГРН) владельца квалифицированного сертификата - для юридического

лица (OID = 1.2.643.100.1);

- идентификационный номер налогоплательщика (далее – ИНН) владельца квалифицированного сертификата - для юридического лица (OID = 1.2.643.3.131.1.1).

К формату СОС, согласно стандарту Х. 509, предъявляются следующие основные требования по составу полей:

- Version – версия формата СОС (опционально);
- Signature – алгоритм подписи СОС;
- Issuer – издатель СОС;
- ThisUpdate – дата выпуска СОС;
- NextUpdate – дата окончания действия СОС (опционально);
- RevokedCertificates – список атрибутов отозванных сертификатов;
- CrlExtensions – расширения СОС.

К основным полям СОС предъявляются следующие требования:

- Поле «Version» должно содержать значение «1» (соответствует версии 2);
- Поле «Issuer» должно содержать DN издателя сертификата;
- Поле «NextUpdate» должно присутствовать.

Кроме того, в СОС должны присутствовать следующие расширения:

- Authority Key Identifier (OID = 2.5.29.35);
- Идентификатор ключа издателя в форме keyIdentifier;
- CRLNumber (OID = 2.5.29.20);
- Номер СОС.

Расширение Delta CRL Indicator (OID = 2.5.29.27) присутствовать не должно, т.к. Система не поддерживает обработку delta-СОС.