**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на выполнение работ по созданию компонента «Управление ключевыми носителями информации»**

# Общие сведения

В рамках выполнения работ Исполнитель должен выполнить работы по созданию компонента «Управление ключевыми носителями информации» (далее – Подсистема) подсистемы сервисов формирования и проверки электронных подписей Комплексной системы обеспечения информационной безопасности в Центральном аппарате (далее – ЦА) Фонда социального страхования Российской Федерации (далее – Фонд).

Сроки выполнения работ: с даты заключения Государственного контракта 90 рабочих дней.

Требования к составу и содержанию работ определяются в разделе 5.

# Назначение Подсистемы

Подсистема предназначена для оптимизации процессов управления жизненным циклом ключевых носителей и ключей электронной подписи за счет реализации следующих методов и средств:

* ведение централизованной базы данных пользователей Подсистемы – владельцев ключей электронной подписи;
* автоматизация процедур генерации ключей и изготовления сертификатов ключей проверки электронной подписи;
* автоматизация процедур управления статусом действия сертификатов ключей проверки электронной подписи;
* ведение журнала учета средств криптографической защиты информации (далее – СКЗИ) в электронном виде.

# Характеристики объекта автоматизации и объекта защиты

Объектом автоматизации является ЦА Фонда, расположенный по адресам:

* г. Москва, Орликов пер., д. 3, корп. А;
* г. Москва, ул. Маши Порываевой д. 11 корп. Б, этаж 14.

Объект автоматизации включает 450 автоматизированных рабочих мест, пользователи которых используют ключи электронной подписи.

Количество пользователей – владельцев ключей электронной подписи – 270.

Объектом защиты является информация, обрабатываемая в информационных системах и передаваемая по каналам связи Фонда.

# Требования к Подсистеме

## Требования к Подсистеме в целом

### Требования к структуре и функционированию Подсистемы

#### Перечень компонент, их назначение

В состав Подсистемы должны входить следующие компоненты:

* комплекс средств централизованного управления жизненным циклом электронной подписи (далее – Комплекс управления).

### Требования к численности работников и функциональным ролям

Подсистема должна поддерживать следующие административные роли:

* Пользователь;
* Оператор;
* Аудитор;
* Администратор информационной безопасности (Администратор ИБ);
* Менеджер запуска плана технического обслуживания.

Численность и квалификация работников, эксплуатирующих Подсистему, должны определяться с учетом следующих требований:

* структура и конфигурация Подсистемы должны быть спроектированы и реализованы с целью минимизации количественного состава обслуживающего персонала;
* структура Подсистемы должна предоставлять возможность как управления всем доступным функционалом Подсистемы одному администратору, так и разделения ответственности по администрированию между несколькими администраторами;
* Подсистема не должна требовать круглосуточного обслуживания и присутствия администраторов у консоли управления.

### Показатели назначения

Подсистема должна предусматривать возможность масштабирования по производительности и объему обрабатываемой информации без модификации ее программного обеспечения путем модернизации используемого комплекса технических средств. Возможности масштабирования должны обеспечиваться средствами технических средств.

Подсистема должна обеспечивать управление жизненным циклом электронной подписи для не менее 450 пользователей.

### Требования к надежности

Подсистема должна удовлетворять следующим требованиям по надежности:

* обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности;
* обеспечивать штатное функционирование в случае одновременной работы всех пользователей на объекте автоматизации;
* обеспечивать возможность интеграции с системой резервного копирования данных Заказчика.

При ошибках, связанных с базовым программным обеспечением (операционной системой и драйверами устройств), восстановление работоспособности должно возлагаться на операционную систему.

Должна быть предусмотрена организация автоматического и/или ручного резервного копирования данных системы компонент Подсистемы средствами системного и базового программного обеспечения, входящего в состав компонент Подсистемы.

### Требования к Исполнителю

Исполнитель должен соответствовать требованиям, установленным законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся объектом закупки (Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности»), а именно, – обладать лицензией на осуществление деятельности по технической защите конфиденциальной информации, выданной Федеральной службой по техническому и экспортному контролю согласно Постановлению Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

## Требования к параметрам, конфигурации, комплектации поставляемых компонентов Подсистемы

### Комплекс средств централизованного управления жизненным циклом электронной подписи

#### Общие требования к Комплексу управления

Комплекс управления должен удовлетворять следующим общим требованиям:

1. поставляться в виде комплекса программного обеспечения и иметь интерфейс управления на русском языке;
2. функционировать в соответствии с архитектурой «клиент-сервер»;
3. поддерживать создание кластера на базе технологии NLB компании Microsoft.

#### Требования к функциональным характеристикам Комплекса

Функциональные характеристики Комплекса управления должны отвечать следующим требованиям:

1. Должна быть обеспечена возможность импорта списка пользователей из каталога Active Directory.
2. Комплекс должен обеспечивать автоматизацию следующих типовых операций по управлению жизненным циклом с ключевых носителей:
	1. регистрация ключевых носителей;
	2. инициализация ключевых носителей;
	3. генерация ключей электронной подписи и запись их на ключевой носитель;
	4. блокировка и разблокировка ключевых носителей;
	5. вывод ключевого носителя из эксплуатации.
3. Должна быть предусмотрена возможность регистрации новых ключевых носителей в пакетном режиме с использованием загружаемых в Комплекс управления информационных файлов, полученных от поставщика ключевых носителей.
4. Должна быть предусмотрена возможность регистрации эксплуатируемых у Заказчика ключевых носителей с сохранением всех ранее выпущенных ключей на ключевом носителе.
5. Комплекс должен иметь возможность передачи запросов на издание сертификатов ключей проверки электронной подписи в центр сертификации Microsoft Active Directory Certificate Services.
6. Комплекс управления должен предоставлять возможность ведения поэкземплярного учета ключевых носителей с предоставлением следующей информации:
	1. серийный номер персонального ключевого носителя;
	2. номер средства защиты информации (далее – СЗИ) или СКЗИ;
	3. перечень объектов (сертификатов и т. д.), размещенных на персональном ключевом носителе.
7. Комплекс управления должен включать агентское программное обеспечение, обеспечивающее применение политик безопасности Комплекса управления для подключенных к автоматизированным рабочим местам с установленным агентским программным обеспечением ключевых носителей.
8. Комплекс управления должен включать агентское программное обеспечение, обеспечивающее реализацию следующих функциональных возможностей:
	1. просмотр сведений о подключенных ключевых носителях пользователя;
	2. разблокировка подключенного ключевого носителя;
	3. генерация ключей и сохранение их на подключенный ключевой носитель пользователя.
9. Комплекс управления должен обеспечивать ролевое разграничение доступа к функциональным возможностям по настройке Комплекса управления.
10. Комплекс управления должен осуществлять аудит действий работников и администраторов в отношении подключенных к техническим средствам с установленным программным обеспечением Комплекса управления ключевых носителей.
11. Комплекс управления должен включать программное обеспечение рабочего места администратора Комплекса управления, обеспечивающее реализацию следующих функциональных возможностей:
	1. регистрация пользователей и рабочих станций в базе данных Комплекса управления;
	2. генерация ключей и сохранение их на ключевые носители пользователей;
	3. настройка профилей выпуска ключевых носителей;
	4. редактирование и назначение роли пользователям Комплекса управления;
	5. выполнение планов обслуживания Комплекса управления.

#### Требования к функциональным ролям Комплекса управления

Комплекс управления должен обеспечивать контроль доступа административных ролей и пользователей к операциям в соответствии с матрицей доступа, приведенной в таблице (Таблица 1).

Таблица 1 — Матрица функциональных ролей Комплекса управления

| **Операция** | **Поль­зова­тель** | **Опера­тор** | **Ауди­тор** | **Адми­нистратор ИБ** | **Запуск плана обслужи­вания** |
| --- | --- | --- | --- | --- | --- |
| **Обслуживание сервера** |
| Администрирование |  | + | + | + |  |
| Старт/Монтирование хранилища аутентификаторов доступа |  | + |  |  |  |
| Стоп/Демонтирование хранилища аутентификаторов доступа |  | + |  |  |  |
| Чтение конфигурации сервера |  | + | + | + |  |
| Изменение конфигурации сервера |  | + |  |  |  |
| Чтение планов обслуживания |  | + | + | + | + |
| Выполнение планов обслуживания |  | + |  |  | + |
| Изменение настроек плана обслуживания |  | + |  |  |  |
| Чтение лицензий |  | + | + | + |  |
| Управление лицензиями |  | + |  |  |  |
| Чтение журнала событий |  | + | + | + |  |
| Запись в журналы событий |  | + |  | + |  |
| Чтение из каталога учетных записей |  | + | + | + |  |
| Управление поставщиками аутентификаторов доступа |  | + |  |  |  |
| Управление перечнем поддерживаемых ключевых носителей |  | + |  | + |  |
| **Основные аутентификаторы доступа** |
| Отзыв основного аутентификатора доступа |  |  |  | + |  |
| Чтение информации об основном аутентификаторе доступа |  | + | + | + |  |
| Резервное копирование основного аутентификатора доступа |  | + |  |  |  |
| Восстановление основного аутентификатора доступа |  | + |  |  |  |
| Смена основного аутентификатора доступа |  |  |  | + |  |
| **Пользователи** |
| Чтение |  | + | + | + |  |
| Регистрация |  |  |  | + |  |
| Удаление |  |  |  | + |  |
| Изменение |  |  |  | + |  |
| Чтение сертификатов пользователя |  | + | + | + |  |
| Регистрация сертификата пользователя |  |  |  | + |  |
| Удаление сертификата пользователя |  |  |  | + |  |
| Чтение сертификатов операторов |  | + | + | + |  |
| Регистрация сертификата оператора |  |  |  | + |  |
| Удаление сертификата оператора |  |  |  | + |  |
| Открытие сеанса пользователя | + |  |  |  |  |
| **Рабочие станции** |
| Чтение |  | + | + | + |  |
| Регистрация |  |  |  | + |  |
| Удаление |  |  |  | + |  |
| Изменение |  |  |  | + |  |
| Чтение операций |  | + | + | + |  |
| **Ключевые носители** |
| Чтение |  | + | + | + | + |
| Изменение |  | + |  | + |  |
| Регистрация ключевого носителя |  | + |  | + |  |
| Назначение пользователю |  | + |  | + |  |
| Выпуск |  | + |  | + |  |
| Удаление |  | + |  | + |  |
| Включение/Отключение |  | + |  | + |  |
| Отзыв |  | + |  | + |  |
| Замена |  | + |  | + |  |
| Возврат в эксплуатацию |  | + |  | + |  |
| Разблокировка |  | + |  | + |  |
| Чтение из УЦ |  |  |  | + |  |
| Чтение объекта на КН |  |  |  | + |  |
| Чтение коннекторов |  |  |  | + |  |
| Синхронизация |  | + |  | + |  |
| **Роли** |
| Чтение |  | + | + | + |  |
| Создание |  |  |  | + |  |
| Удаление |  |  |  | + |  |
| Изменение |  |  |  | + |  |
| Управление членством роли |  |  |  | + |  |
| **Глобальные группы** |
| Чтение |  | + | + | + | + |
| Создание |  |  |  | + |  |
| Удаление |  |  |  | + |  |
| Изменение |  |  |  | + |  |
| Управление членством глобальной группы |  |  |  | + |  |
| **Профили** |
| Чтение типов профилей |  | + | + | + |  |
| Чтение экземпляров профилей |  | + | + | + |  |
| Добавление нового типа профиля |  |  |  | + |  |
| Добавление нового экземпляра профиля |  |  |  | + |  |
| Изменение экземпляра профиля |  |  |  | + |  |
| Удаление экземпляра профиля |  |  |  | + |  |
| Управление привязкой профиля |  |  |  | + |  |
| **Приложения** |
| Чтение |  | + | + | + |  |
| Регистрация |  |  |  | + |  |
| **Категории событий** |
| Чтение |  | + | + | + |  |
| Регистрация |  |  |  | + |  |

#### Требования к аппаратному обеспечению Комплекса управления

Программное обеспечение Комплекса управления должно обеспечивать реализацию заданных настоящим Техническим заданием функциональных требований при работе на аппаратном обеспечении, удовлетворяющем следующим минимальным характеристикам:

1. свободное дисковое пространство технических средств, предназначенных для функционирования серверных компонентов Комплекса управления: не менее 25 Гб;
2. объем оперативной памяти технических средств, предназначенных для функционирования серверных компонентов Комплекса управления: не менее 4 Гб;
3. свободное дисковое пространство технических средств, предназначенных для функционирования программного обеспечения администрирования: не менее 100 Мб;
4. свободное дисковое пространство технических средств, предназначенных для функционирования агентского программного обеспечения: не менее 30 Мб.

#### Требования к основному программному обеспечению Комплекса управления

Программное обеспечение Комплекса управления должно удовлетворять следующим требованиям:

1. Серверная часть Комплекса управления должна функционировать под управлением операционных систем:
	1. Microsoft Windows Server 2008 R2 SP1;
	2. Microsoft Windows Server 2012 R2.
2. Серверная часть Комплекса управления должна обеспечивать хранение собственной базы данных в СУБД:
	1. Microsoft SQL Server 2012.
3. Клиентская часть Комплекса управления и рабочая станция администратора должны функционировать под управлением операционных систем:
	1. Windows 8;
	2. Windows 8.1 (32/64-бит);
	3. Windows 7 SP1 (32/64-бит);
	4. Windows XP SP3 (32-бит);
	5. Windows Server 2012 R2;
	6. Windows Server 2012;
	7. Windows Server 2008 R2 SP1;
	8. Windows Server 2008 SP2 (32/64-бит).
4. Комплекс управления должен обеспечивать регистрацию следующих событий:
	1. создание и удаление административных ролей;
	2. попытка монтирования/демонтирования хранилища аутентификаторов доступа;
	3. блокировка и разблокировка рабочей станции;
	4. добавление и удаление рабочей станции;
	5. удаление, добавление, регистрация и блокировка пользователя;
	6. регистрация и удаление сертификатов пользователя и оператора;
	7. отзыв, смена и восстановление основного аутентификатора доступа.
5. Для каждого из вышеуказанных событий должна регистрироваться следующая информация:
	1. дата и время выполняемого действия;
	2. субъект, осуществляющий регистрируемое действие;
	3. тип события.
6. Комплекс управления должен обеспечивать возможность выборочного ознакомления с регистрационной информацией на основе следующих параметров:
	1. тип регистрируемого события;
	2. период регистрации событий.

#### Прочие требования к Комплексу

Тип лицензирования Комплекса управления должен быть на основе количества пользователей, ключевыми носителями которых может управлять Комплекс управления.

Гарантийный срок на Комплекс управления должен составлять не менее 12 (двенадцати) месяцев. В течение гарантийного срока поставщиком (разработчиком) должна осуществляться техническая поддержка, включая предоставление необходимой технической информации о Комплексе управления, проведение консультаций по вопросам, связанным с функционированием программного обеспечения Комплекса управления.

Программное обеспечение Комплекса управления должно быть сертифицировано по требованиям безопасности информации на соответствие требованиям следующего документа: «Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Гостехкомиссия России, 1999 г.» по уровню контроля не ниже 4.

Программное обеспечение Комплекса управления должно соответствовать требованиям, установленным постановлением Правительства Российской Федерации от 16.11.2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» по классам программного обеспечения в соответствии с классификатором, утвержденным приказом Минкомсвязи России от 01.04.2016 № 134: 02.11 «Системы мониторинга и управления» и 02.13 «Средства обеспечения информационной безопасности».

# Состав и содержание работ

Исполнитель должен выполнить следующие работы:

1. передача Заказчику программного обеспечения Подсистемы;
2. сбор исходных данных для проектирования и внедрения Подсистемы;
3. технический проект и рабочая документация;
4. монтажные и пусконаладочные работы;
5. инструктаж ответственных работников ЦА Фонда по администрированию Подсистемы.

Адрес поставки программного обеспечения: г. Москва, Орликов пер., д. 3, корп. А.

Адреса установки программного обеспечения приведены в разделе 3 настоящего документа.

Состав и содержание работ, перечень документов, предъявляемых по окончании работ, приведены в таблице (Таблица 2).

Таблица 2 — Состав и содержание работ, перечень документов

| **№** | **Описание производимых работ** | **Результат выполнения работ** |
| --- | --- | --- |
| 1 | Сбор исходных данных для проектирования и внедрения Подсистемы | Проведено обследование ИТ-инфраструктуры ЗаказчикаОпределены требования к Подсистеме, ее интеграции со смежными системами и ИТ-инфраструктурой ЗаказчикаРазработан документ Техническое задание |
| 2 | Технический проект и рабочая документация | Разработана архитектура Подсистемы.Разработана организационная структура Подсистемы.Определены требования к площадкам внедрения и смежным подсистемам.Определен состав мероприятий по подготовке площадок внедрения к монтажным и пусконаладочным работамРазработаны документы:* План внедрения
* Комплект рабочей документации, приведенный в пунктах 1−4 таблицы 4
* Комплект эксплуатационных документов, приведенных в пунктах 5−8 таблицы 4
 |
| 3 | Монтажные и пусконаладочные работы | Выполнена установка и настройка системного программного обеспечения на аппаратное обеспечение сервера, предоставленное Заказчиком.Выполнена установка и настройка специального программного обеспечения Подсистемы на сервер Подсистемы и АРМ обслуживающего персонала.Проведены испытания Подсистемы.Разработаны документы:* Рабочий журнал опытной эксплуатации;
* Протокол приемочных испытаний
 |
| 4 | Инструктаж ответственных работников ЦА Фонда по администрированию Подсистемы | Проведен инструктаж персонала Подсистемы в объеме, необходимом для выполнения обязанностей по обслуживанию Подсистемы, регистрации пользователей и ключевых носителей, изготовлению ключей ЭП и сертификатов ключей проверки ЭП.Протокол подготовки персонала |

Перечень разрабатываемых документов приведен в таблице (Таблица 3).

Таблица 3 — Перечень документов комплекта рабочей документации

| **№** | **Наименование документа** | **Код документа** |
| --- | --- | --- |
|  | Ведомость рабочей документации | РД |
|  | Схема структурная Комплекса технических средств | С1 |
|  | Спецификация оборудования и программного обеспечения | В4 |
|  | Программа опытной эксплуатации | ПМ |
|  | Программа и методика испытаний | ПМ |
|  | **Эксплуатационная документация** |  |
|  | Ведомость эксплуатационной документации | ЭД |
|  | Руководство пользователя | И3 |
|  | Руководство по администрированию | ИА |
|  | Инструкция по эксплуатации комплекса технических средств  | ИЭ |

Документация на Подсистему должна содержать сведения, необходимые для обеспечения выполнения работ по обслуживанию Комплекса, а также для поддержания уровня эксплуатационных характеристик компонент Комплекса в соответствии с принятыми проектными решениями (см. п. 4.2).

Документация согласно таблице 3 предоставляется Исполнителем в печатном виде (2 экземпляра) и в электронном виде на материальном носителе в формате PDF.

Монтажные и пусконаладочные работы выполняются на площадках, адреса которых приведены в разделе 3 настоящего документа. Технические средства для установки программного обеспечения предоставляет Заказчик. Регистрацию и выдачу ключевых носителей пользователям Подсистемы выполняет Заказчик.

Состав группы ответственных работников Фонда (не более 5 человек) для прохождения подготовки персонала определяется Заказчиком и предоставляется Исполнителю после заключения Государственного контракта.

В случае необходимости по требованию Заказчика Исполнитель предоставляет презентацию хода исполнения Государственного контракта.

# Порядок контроля и приемки

* 1. ***Порядок оформления и предъявления Заказчику результатов работ***

Подсистема должна быть передана в виде установленного на предоставленное Заказчиком аппаратное обеспечение функционирующего программного обеспечения в сроки, предусмотренные Государственным контрактом. Приемка результатов работ должна осуществляться комиссией в составе уполномоченных представителей Заказчика и Исполнителя в соответствии с документом «Программа и методика испытаний».

* 1. ***Виды, состав, объем и методы испытаний Комплекса***

Испытания Подсистемы должны включать два этапа:

* опытная эксплуатация в течение 10 рабочих дней (далее – ОЭ);
* приемочные испытания.

Объем, методы и порядок проведения ОЭ должны определяться Программой опытной эксплуатации. До начала ОЭ Исполнитель должен передать Заказчику полный набор учетных записей, паролей и других параметров доступа к Подсистеме. В течение опытной эксплуатации Исполнитель обеспечивает консультацию работников Заказчика по телефону и электронной почте. Результаты проведения ОЭ должны быть зафиксированы в Рабочем журнале опытной эксплуатации.

Объем, методы и порядок проведения приемочных испытаний должны определяться Программой и методикой испытаний. По результатам приемочных испытаний оформляется протокол проведения приемочных испытаний.

* 1. ***Общие требования к приемке работ***

Сдача-приемка работ должна производиться в соответствии с Государственным контрактом и Программой и методикой испытаний.

# Требования к гарантийному обслуживанию

Срок действия гарантии Исполнителя на создаваемую Подсистему должен составлять не менее 12 (двенадцати) месяцев с даты подписания акта о приемке выполненных работ.

Срок действия гарантии на поставляемые компоненты Подсистемы должен составлять не менее 12 (двенадцати) месяцев с даты подписания акта о приемке выполненных работ.

Комплектующие, которые Исполнитель устанавливает на компоненты подсистем в течение гарантийного периода при восстановлении его работоспособности, должны быть произведены теми же производителями, что и исходные комплектующие.

В гарантийный период устранение обнаруженных неисправностей компонент Подсистемы должно быть выполнено в течение 20 (двадцати) рабочих дней со дня получения от Заказчика уведомления о выявлении дефекта(ов) и/или неисправности(ей) и/или несоответствий компонент Подсистемы.

В случае необходимости выполнения работ по гарантийному ремонту компонент Подсистемы не в месте размещения компонент Подсистемы их транспортировка до места гарантийного ремонта и обратно должна осуществляться силами и за счет Исполнителя.

В случае невозможности восстановления работоспособности неисправной компоненты Подсистемы в вышеуказанные сроки Исполнитель должен предоставить на время восстановления работоспособности аналогичный по функциональным характеристикам компонент, провести работы по его установке и настройке.