

УТВЕРЖДАЮ

Заместитель руководителя
Федерального казначейства


_____ А.С. Албычев
« 06 » 10 2020 г.

**РЕГЛАМЕНТ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ПОДСИСТЕМАМ
СИСТЕМЫ УПРАВЛЕНИЯ ЭКСПЛУАТАЦИЕЙ ФЕДЕРАЛЬНОГО
КАЗНАЧЕЙСТВА**

СОГЛАСОВАНО

От Федерального казначейства
Начальник Управления
информационной инфраструктурой


_____ И. В. Кальченко
« 05 » 10 2020 г.

Москва, 2020

Оглавление

1. Сокращения и определения	3
1.1. Сокращения	3
1.2. Определения	4
2. Общие положения	7
3. Формирование Заявки на предоставление доступа	8
4. Регламентное время обработки Заявки	9
5. Аутентификация и авторизация Пользователей	11
6. Требования к сертификатам ключа аутентификации и шифрования	12
7. Ролевая модель доступа	13
7.1. Объекты доступа и права доступа для ролей в ПУПЭ	13
7.2. Объекты доступа и права доступа для ролей в ПХКЭ	15
7.3. Объекты доступа и права доступа для ролей в ПУМИ/ПУМС	16
7.4. Объекты доступа и права доступа для ролей в ПИО	17
7.5. Объекты доступа и права доступа для ролей в ПЕКЦ	19
8. Обеспечение безопасности информации при доступе Пользователей к подсистемам СУЭ	20
8.1. Организационные меры безопасности	21
8.2. Технические меры безопасности	22
8.2.1. Обеспечение безопасности на АРМ Пользователя	22
8.2.2. Обеспечение защищенного подключения	23
Приложение	24

1. Сокращения и определения

В настоящем Регламенте предоставления доступа к подсистемам Системы управления эксплуатацией Федерального казначейства (далее – Регламент) используются следующие сокращения и определения:

1.1. Сокращения

АРМ	Автоматизированное рабочее место
АПКШ	Аппаратно-программный комплекс шифрования
ИБ	Информационная безопасность
ИС	Информационная система
ЗКВС	Защищенный контур вычислительной сети
МНИ	Машинный носитель информации
ОрФК	Центральный аппарат Федерального казначейства, территориальный орган Федерального казначейства, ФКУ «ЦОКР»
ПЕКЦ	Подсистема единый контактный центр СУЭ
ПНО	Подсистема информирования и отчетности СУЭ
ПО	Программное обеспечение
ПУМИ	Подсистема управления и мониторинга инфраструктуры СУЭ
ПУМС	Подсистема управления и мониторинга сервисов СУЭ
ПУПЭ	Подсистема управления процессами эксплуатации СУЭ
ПХКЭ	Подсистема хранения конфигурационных элементов СУЭ

СУЭ	Система управления эксплуатацией Федерального казначейства
ФК	Федеральное казначейство
ФКУ «ЦОКР»	Федеральное казенное учреждение «Центр по обеспечению деятельности Казначейства России»

1.2. Определения

Информационный сервис ФК	Логически объединенная и понятная пользователям ИС совокупность функциональных областей, функций и структурных модулей, поддерживаемых прикладным программным обеспечением и входящих в состав ИС, обеспечивающая выполнение пользователями функциональных задач
Исполнитель	Юридическое лицо, заключившее с Заказчиком государственный контракт на выполнение работ по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации ИС ОрФК или выполняющее работы в рамках гарантийных обязательств, предусмотренных Государственным контрактом
Контактное лицо Исполнителя	Лицо, уполномоченное Исполнителем на решение оперативных вопросов с Заказчиком по предоставлению, блокировке, аннулированию доступов, блокировке и отзыву сертификатов ключей аутентификации и шифрования. Указывается в Заявке на предоставление доступа
Эксплуатация СУЭ	Использование функционала СУЭ, в том числе функционала для работы с заявками в ПУПЭ, в рамках выполнения обязательств по государственным контрактам на выполнение работ по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации ИС ОрФК, а также использование функционала СУЭ в

	рамках гарантийных обязательств, предусмотренных государственным контрактом
Ответственный за эксплуатацию	Подразделения, ответственные за эксплуатацию подсистем СУЭ (менеджеры ИТ-сервиса)
Заказчик	ФК, ФКУ «ЦОКР»
Пользователь	Сотрудник Исполнителя, сотрудник ОрФК, для которого запрашивается и которому предоставляется доступ к подсистемам СУЭ из внешней сети
Администратор ИБ	Сотрудник, ответственный за обеспечение и контроль доступа Исполнителей к ИС ОрФК
Запрос на сертификат ключа аутентификации и шифрования	Файл, созданный с использованием криптографических средств, содержащий ключ проверки закрытого ключа аутентификации и шифрования и иную информацию об Исполнителе
Сертификат ключа аутентификации и шифрования	Электронный документ, сформированный Администратором ИБ Заказчика на основании запроса на генерацию, предоставленного Исполнителем, и подтверждающий принадлежность закрытого ключа аутентификации и шифрования владельцу сертификата ключа аутентификации и шифрования
Закрытый ключ аутентификации и шифрования	Уникальная последовательность символов, предназначенная для аутентификации Исполнителя на стороне Федерального казначейства с последующим установлением защищенного (шифрованного) канала связи
Компрометация закрытого ключа аутентификации и шифрования	Ознакомление неуполномоченного лица (лиц) с закрытым ключом аутентификации и шифрования; случаи, когда невозможно достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не

	опровергнута возможность того, что данный факт произошел в результате действий злоумышленника)
Сервер доступа	Программное обеспечение, установленное на АПКШ и предназначенное для авторизации сессий доступа

2. Общие положения

Регламент определяет порядок действий, необходимых для подключения Пользователей к СУЭ в качестве потребителей, эксплуатирующих ее функциональные возможности.

Реализация доступа к подсистемам СУЭ позволяет Пользователям эксплуатировать подсистемы СУЭ, размещенные в ЗКВС.

Регламент определяет порядок получения Пользователями доступа к подсистемам СУЭ при подключении к ним из сети Интернет.

Исполнителю предоставляется доступ к подсистемам СУЭ на основании действующего Государственного контракта, предусматривающего оказание услуг / проведение работ по созданию, развитию, вводу в эксплуатацию, эксплуатации, выводу из эксплуатации ИС ФК, и / или при необходимости исполнения гарантийных обязательств в рамках Государственного контракта и с соблюдением всех предусмотренных им условий.

При необходимости предоставления доступа к СУЭ Пользователям субподрядной организации, привлеченной Исполнителем к оказанию предусмотренных Государственным контрактом услуг, Заявку на предоставление доступа в СУЭ для Пользователей субподрядной организации оформляет Исполнитель. При этом (за исключением оформления Заявки на предоставление доступа) на субподрядную организацию и ее Пользователей распространяются положения Регламента в части, касающейся требований и правил, предъявляемых к Исполнителю и его Пользователям, включая требования к ознакомлению с Регламентом и соблюдению требований информационной безопасности.

Требования об обязательности выполнении Исполнителями условий Регламента включаются в тексты Государственных контрактов, предусматривающих доступ сотрудников Исполнителей к подсистемам СУЭ.

С Регламентом обязаны ознакомиться под расписку Пользователи следующий категорий:

- Все Пользователи (Сотрудники Исполнителя и сотрудники ОрФК), доступ которым к подсистемам СУЭ ФК предоставляется из сети Интернет;
- Сотрудники ОрФК, принимающие непосредственное участие в процессах согласования и предоставления доступов.

3. Формирование Заявки на предоставление доступа

Доступ к СУЭ предоставляется Исполнителю на основании Заявки на предоставление доступа к подсистемам СУЭ и выдачу сертификатов ключей аутентификации и шифрования (далее – Заявка), содержащую сведения о Контактном лице Исполнителя, Пользователях, сроках предоставления доступа, перечень подсистем СУЭ, сетевых протоколах, сетевых адресах и другие данные по форме, представленной в Приложении к Регламенту.

При заполнении столбца с информацией о подсистемах, к которым Исполнителем запрашивается доступ, необходимо указывать одну или несколько (при необходимости) подсистем СУЭ. Параметры подсистем указаны в качестве примера в Приложении к Заявке.

К Заявке Исполнителю необходимо прикладывать Каталог ИТ-сервиса в соответствии с шаблоном Каталога ИТ-сервиса, входящего в состав документа «Требования к перечню и составу документации, исходным кодам и дистрибутивам информационных систем, сдаваемых в Фонд алгоритмов и программ Федерального казначейства», размещенного на официальном сайте Федерального казначейства в сети Интернет в подразделе ГИС/Документы (<http://www.roskazna.ru/gis/dokumenty/>).

Необходимым условием для рассмотрения Заявки от Исполнителя является полное заполнение Заявки с приложенным Каталогом ИТ-сервиса, подписание Заявки уполномоченным лицом Исполнителя и направление ее в адрес Директора ФКУ «ЦОКР».

Необходимым дополнительным условием для рассмотрения Заявки от Исполнителя, включающей в себя Пользователей субподрядной организации, является приложение к Заявке копии договора между Исполнителем и субподрядной организацией на оказание услуг / выполнение работ, осуществляемых Исполнителем в рамках Государственного контракта.

Необходимым условием для рассмотрения Заявки на предоставление доступа сотрудникам ОрФК является заполнение Заявки, подписанной руководителем подразделения ОрФК, и ее направление в адрес Директора ФКУ «ЦОКР». При этом в Заявке вместо информации о Государственном контракте необходимо обосновать предоставление доступа из сети Интернет.

К Заявке также должен прилагаться МНИ, содержащий файлы запросов на сертификаты ключей аутентификации и шифрования на всех Пользователей, указанных в Заявке.

Процедура генерации запроса на сертификаты ключей аутентификации и шифрования и требования к запросам на сертификаты ключей аутентификации и шифрования изложены в «Инструкции по настройке и подключению АРМ Пользователя к Системе управления эксплуатацией».

4. Регламентное время обработки Заявки

Началом времени обработки Заявки на предоставление доступа является дата ее поступления и регистрации Заказчиком.

Процедура обработки Заявки включает в себя следующие этапы:

- регистрацию у Заказчика в качестве входящей корреспонденции;
- согласование ответственными подразделениями Заказчика на предмет корректности заполнения и данных;
- исполнение ответственными подразделениями Заказчика, включая выпуск сертификатов ключей аутентификации и шифрования;

- уведомление инициатора Заявки о предоставлении доступа в соответствии с поступившей Заявкой.

Общий срок обработки Заявки составляет: 10 рабочих дней¹.

В процессе обработки Заявки при условии успешного прохождения процедуры ее согласования у Заказчика на адреса электронной почты Пользователей, указанных в Заявке, будут направлены сертификаты ключа аутентификации и шифрования, предназначенные для их регистрации в программном комплексе «Континент-АП».

Пользователь имеет возможность приступить к подключению АРМ к СУЭ из сети Интернет с момента получения уведомления о предоставлении доступа.

При несоответствии поступившей Заявки требованиям, предусмотренным разделом 3 Регламента, Заявка подлежит отклонению. В этом случае в адрес Исполнителя или Пользователя – сотрудника ОрФК будет направлено официальное письмо с указанием причины отказа в исполнении ранее поступившей Заявки.

При наличии вопросов по содержанию поступившей Заявки, требующих уточнения со стороны Исполнителя, Заказчик может направить посредством электронной почты в адрес Контактного лица Исполнителя или Пользователя – сотрудника ОрФК уточняющий запрос, по результату рассмотрения ответа на который, Заказчик принимает решение об исполнении или отклонении Заявки. В случае отсутствия ответа Исполнителя или Пользователя – сотрудника ОрФК в течение двух рабочих дней с даты получения уточняющего запроса со стороны Заказчика Заявка признается несоответствующей требованиям, предусмотренным разделом 3 Регламента.

¹ При объеме запрошенных в рамках одной Заявки сертификатов не более 50 штук. В случае превышения порога в 50 штук срок исполнения заявки увеличивается на 5 рабочих дней

5. Аутентификация и авторизация Пользователей

Получение доступа к подсистемам СУЭ ФК предусматривает прохождение Пользователем СУЭ ФК процедур аутентификации и авторизации.

Аутентификация в СУЭ ФК Пользователей осуществляется с применением действующих сертификатов ключей аутентификации средства криптографической защиты информации (далее – СКЗИ) «Континент-АП».

СКЗИ «Континент-АП» включает в свой состав компоненты, обеспечивающие доступ пользователей к ресурсам СУЭ в ЗКВС с АРМ Пользователя, расположенного за пределами ЗКВС. На АРМ Пользователя устанавливается СКЗИ «Континент-АП», который для передачи данных соединяется Сервером доступа, проверяющим полномочия на доступ и разрешающим доступ к СУЭ, размещенной в ЗКВС.

АРМ Пользователя должно удовлетворять всем требованиям, предъявляемым к аппаратному и программному обеспечению, изложенным в «Инструкции по настройке и подключению АРМ Пользователя к Системе управления эксплуатацией».

После прохождения процедуры аутентификации производится авторизация Пользователя в СУЭ.

Авторизация действий пользователей осуществляется с использованием встроенных в СУЭ механизмов авторизации в соответствии с Ролевой моделью доступа (раздел 6 Регламента) к подсистемам СУЭ.

Для авторизации Пользователей в СУЭ применяются два основных параметра: логин и соответствующий ему пароль доступа, которые предоставляются Пользователям на основании согласованной Заявки в соответствии с требованиями Регламента.

Присвоенные Пользователю логин и пароль доводятся до Пользователя способом, исключающим возможность ознакомления с ними иных лиц.

6. Требования к сертификатам ключа аутентификации и шифрования

Срок действия сертификата ключа аутентификации и шифрования определяется условиями Государственного контракта, в целях исполнения которого, запрашивается доступ к подсистемам СУЭ, или сроком, необходимым для исполнения гарантийных обязательств.

Срок действия сертификата ключа аутентификации и шифрования не может превышать максимально допустимый срок действия закрытого ключа аутентификации и шифрования, установленный эксплуатационной документацией для используемого СКЗИ.

В случае окончания срока действия сертификата ключа аутентификации и шифрования ранее, чем требуемый срок предоставления удаленного доступа (не превышая при этом сроки, определенные Государственным контрактом, в целях исполнения, которого запрашивается удаленный доступ к подсистемам СУЭ), Исполнитель направляет в адрес Заказчика Заявку в соответствии с требованиями Регламента.

Внесение изменений в перечень Исполнителей осуществляется путем направления Заказчику новой Заявки.

В случае необходимости приостановить действие / отозвать сертификат ключа аутентификации и шифрования Пользователя, не связанной с компрометацией закрытого ключа аутентификации и шифрования, например, при прекращении трудовых обязательств Пользователя, Исполнитель должен направить Заказчику письмо с объяснением причин блокировки, предварительно направив с электронного почтового адреса Контактного лица Исполнителя соответствующее письмо на почтовый ящик *rud@roskazna.ru*.

Если Государственным контрактом предусмотрены сроки выполнения по видам работ, время, затраченное на организацию удаленного доступа, не

включается в общее время реагирования на инцидент. Информация о времени, затраченном на обработку заявки на выполнение работ, содержится в СУЭ.

7. Ролевая модель доступа

7.1. Объекты доступа и права доступа для ролей в ПУПЭ

На объекты ПУПЭ Группой поддержки СУЭ настраивается доступ «Группам поддержки» со следующими правами в соответствии с Таблицей 1:

Таблица 1

Тип права доступа	Кода типа права доступа	Полномочия
Просмотр	П	Поиск и просмотр информации по объектам
Редактирование в рамках своей группы поддержки	РРГ	Изменение полей в объектах, если объект относится к группе поддержки
Редактирование	Р	Изменение полей в объектах
Нет	Н	Без права доступа

Объекты доступа в ПУПЭ описаны в Таблице 2.

Таблица 2

Инцидент/Задача по инциденту (IM)
Карточка контакта
Обращение (SD)
Проблема (PM)
Карточка организации
Конфигурационный элемент (CI)
Запрос на изменение (RFC/C)
Рабочее задание (T)
Статья Базы знаний (KM)

Права доступа для ролей в ПУПЭ описаны в Таблице 3.

Таблица 3

Роль	Объект системы	Код типа права доступа
Диспетчер	Инцидент/Задача по инциденту	П, Р
	Карточка контакта	П, Р
	Обращение	П, РРГ
	Проблема	П
	Карточка организации	П
	Конфигурационный элемент	П
	Запрос на изменение	П
	Рабочее задание	П, РРГ
	Статья Базы знаний	П
Менеджер инцидентов	Инцидент/Задача по инциденту	П, Р
	Карточка контакта	П, Р
	Обращение	П, Р
	Проблема	П, РРГ
	Карточка организации	П, Р
	Конфигурационный элемент	П
	Запрос на изменение	П
	Рабочее задание	П, РРГ
	Статья Базы знаний	П
Менеджер по Проблемам	Инцидент/Задача по инциденту	П, РРГ
	Карточка контакта	П
	Обращение	П
	Проблема	П, РРГ, Р
	Карточка организации	П
	Конфигурационный элемент	П
	Запрос на изменение	П
	Рабочее задание	П
	Статья Базы знаний	П
Эксперт	Инцидент/Задача по инциденту	П, Р
	Карточка контакта	П, Р
	Обращение	П, РРГ
	Проблема	П, РРГ
	Карточка организации	П, Р
	Конфигурационный элемент	П

	Запрос на изменение	П
	Рабочее задание	П, РРГ
	Статья Базы знаний	П, РРГ
Специалист (специалист 2 и/или 3 линии поддержки)	Инцидент/Задача по инциденту	П, РРГ
	Карточка контакта	П
	Обращение	П
	Проблема	П, РРГ
	Карточка организации	П
	Конфигурационный элемент	П
	Запрос на изменение	П
	Рабочее задание	П, РРГ
	Статья Базы знаний	П
Лидер Команды	Инцидент/Задача по инциденту	П, РРГ
	Карточка контакта	П
	Обращение	П
	Проблема	П, РРГ
	Карточка организации	П
	Конфигурационный элемент	П
	Запрос на изменение	П
	Рабочее задание	П, РРГ
	Статья Базы знаний	П, РРГ
Пользователь	Инцидент/Задача по инциденту	П
	Карточка контакта	Н
	Обращение	П
	Проблема	Н
	Карточка организации	Н
	Конфигурационный элемент	Н
	Запрос на изменение	П
	Рабочее задание	Н
	Статья Базы знаний	Н

7.2. Объекты доступа и права доступа для ролей в ПХКЭ

На объекты ПХКЭ настраивается доступ пользователям со следующими правами в соответствии с Таблицей 4.

Таблица 4

Тип права доступа	Код типа права доступа	Полномочия
Полный доступ	ПП	Все права в системе
Просмотр	П	Поиск и просмотр информации по объектам
Редактирование	Р	Изменение полей в объектах
Нет	Н	Без права доступа

Объекты доступа в ПХКЭ описаны в Таблице 5.

Таблица 5

Конфигурационный элемент (КЭ)
ИТ-актив

Права доступа для ролей в ПХКЭ СУЭ описаны в Таблице 6.

Таблица 6

Роль	Объект системы	Код типа права доступа
Учётчик	КЭ	П, Р
	ИТ-актив	П, Р
Заведующий складом	КЭ	Н
	ИТ-актив	П, Р
Менеджер конфигураций	КЭ	П, Р
	ИТ-актив	П, Р
Администратор ПХКЭ	КЭ	ПП
	ИТ-актив	ПП

7.3. Объекты доступа и права доступа для ролей в ПУМИ/ПУМС

На объекты ПУМИ и ПУМС настраивается доступ пользователям со следующими правами в соответствии с Таблицей 7:

Таблица 7

Тип права доступа	Код типа права доступа	Полномочия
Полный доступ	ПП	Все права в системе

Просмотр	П	Поиск и просмотр информации по объектам
Редактирование	Р	Редактирование параметров

Права доступа для ролей в ПУМИ/ПУМС СУЭ описаны в Таблице 8.

Таблица 8

Роль	Объект системы	Код типа права доступа
Администраторы	Представления	ПП
	Меню администратора	ПП
	Отчеты	ПП
Менеджер событий (Менеджер мониторинга)	Представления	ПП
	Меню администратора	П, Р
	Отчеты	ПП
Специалист ВСО (диспетчер ВСО)	Представления	П
	Отчеты	П

7.4. Объекты доступа и права доступа для ролей в ПИО

На ПИО настраивается доступ пользователя со следующими правами в соответствии с таблицей 9.

Таблица 9

Тип права доступа	Кода типа права доступа	Полномочия
Просмотр	П	Просмотр и выгрузка готовых отчетов по подписке
Создание и Редактирование	СР	Создание отчетов, изменение полей в объектах
Публикация и рассылка по графику	ПРГ	Формирование и сохранение публикаций

Администрирование	А	Администрирование ППО, создание УЗ, создание отчетов
Нет	Н	Без права доступа

Объекты доступа в ППО описаны в Таблице 10.

Таблица 10

Готовая отчетность
Новый отчет
Новая УЗ
Администрирование ППО

Права доступа для ролей в ППО описаны в Таблице 11.

Таблица 11

Роль	Объект системы	Код типа права доступа
Пользователь	Готовая отчетность	П
	Новый отчет	Н
	Новая УЗ	Н
	Администрирование ППО	Н
Дизайнер отчетов	Готовая отчетность	П, СР, А, ПРГ
	Новый отчет	П, СР, А
	Новая УЗ	Н
	Администрирование ППО	Н
Администратор	Готовая отчетность	П, СР, А, ПРГ
	Новый отчет	П, СР, А

	Новая УЗ	П, СР, А
	Администрирование ППО	П, СР, А

7.5. Объекты доступа и права доступа для ролей в ПЕКЦ

На объекты ПЕКЦ настраивается доступ пользователям со следующими правами в соответствии с Таблицей 12:

Таблица 12

Тип права доступа	Код типа права доступа	Полномочия
Полный доступ	ПП	Все права в системе
Просмотр / прослушивание	П	Поиск и просмотр информации по объектам / прослушивание записей телефонных вызовов
Редактирование	Р	Редактирование параметров

Права доступа для ролей в ПЕКЦ описаны в Таблице 13.

Таблица 13

Роль	Объект системы	Код типа права доступа
Администратор	Представления	ПП
	Меню администратора	ПП
	Управление качеством	ПП
	Проекты	ПП
	Отчеты	ПП
	Звукозаписи вызовов	ПП
	Управление вызовами	ПП
	Обработка вызовов	ПП
Менеджер по качеству	Представления	П, Р
	Меню администратора	Н
	Управление качеством	ПП
	Проекты	Н
	Отчеты	П

	Звукозаписи вызовов	П
	Управление вызовами	Н
	Обработка вызовов	Н
Менеджер проекта	Представления	ПП
	Меню администратора	Н
	Управление качеством	Н
	Проекты	ПП
	Отчеты	ПП
	Звукозаписи вызовов	Н
	Управление вызовами	Н
	Обработка вызовов	Н
Супервизор	Представления	П
	Меню администратора	Н
	Управление качеством	Н
	Проекты	П
	Отчеты	П
	Звукозаписи вызовов	Н
	Управление вызовами	ПП
	Обработка вызовов	ПП
Оператор	Представления	Н
	Меню администратора	Н
	Управление качеством	Н
	Проекты	П
	Отчеты	Н
	Звукозаписи вызовов	Н
	Управление вызовами	Н
	Обработка вызовов	ПП

8. Обеспечение безопасности информации при доступе Пользователей к подсистемам СУЭ

Обеспечение безопасности информации при доступе Пользователей к подсистемам СУЭ включает следующие меры безопасности:

- организационные;
- технические;

- контроль за исполнением работ.

Исполнитель подтверждает выполнение мер по обеспечению безопасности информации, изложенных в Регламенте, и обязуется выполнять их весь срок действия Государственного контракта, гарантийных обязательств, в целях исполнения которых предоставляется доступ. Информация об этом направляется официальным письмом в адрес Заказчика до начала работ, предусматривающих доступ к СУЭ.

При доступе к подсистемам СУЭ Пользователя – сотрудника ОрФК обязанность выполнения и соблюдения мер по обеспечению безопасности информации, изложенных в настоящем Регламенте, возлагается на самого Пользователя.

8.1. Организационные меры безопасности

При доступе Пользователей к подсистемам СУЭ должны выполняться следующие требования по организации работ:

- обязательным условием для эксплуатации подсистем СУЭ является наличие в Государственном контракте, в целях исполнения которого предоставляется доступ, пунктов, предусматривающих обязанности и ответственность Исполнителя за обеспечение конфиденциальности и выполнения требований по безопасности информации, предусмотренных законодательством Российской Федерации, нормативными правовыми актами органов государственной власти, нормативных документов Федерального казначейства, регулирующими отношения в области защиты информации. При доступе Пользователей к подсистемам СУЭ должны выполняться следующие требования по организации работ:

- Пользователь обязан блокировать АРМ, с которого осуществляется удаленный доступ, в случае покидания рабочего места;

– не допускается работа нескольких Пользователей под одной учетной записью;

– в случае компрометации закрытого ключа аутентификации и шифрования Контактное лицо Исполнителя / Пользователь – сотрудник ОрФК обязаны незамедлительно уведомить Администратора ИБ средствами электронной почты, отправив письмо на почтовый ящик *rud@roskazna.ru* для оперативной блокировки сессии и удаления сертификатов с серверов доступа. При этом Исполнитель обязан также направить в ФКУ «ЦОКР» официальное письмо о необходимости аннулирования доступа и удаления сертификата ключа аутентификации и шифрования с указанием в письме результатов проведенной Исполнителем проверки причин компрометации закрытого ключа аутентификации и шифрования и мер, принятых для исключения повторения подобных нарушений в дальнейшем. Для восстановления удаленного доступа Пользователя Исполнитель должен направить повторную Заявку в соответствии с требованиями Регламента.

8.2. Технические меры безопасности

Технические меры должны включать соблюдение требований обеспечения безопасности информации:

– при работе на АРМ Пользователя;

– в процессе выполнения всех видов работ и эксплуатации подсистем СУЭ с использованием предоставляемого доступа.

8.2.1. Обеспечение безопасности на АРМ Пользователя

Для АРМ Пользователя должны выполняться следующие требования:

– должны применяться сертифицированные средства защиты информации и СКЗИ;

– должны применяться сертифицированные средства антивирусной защиты;

– должны применяться средства блокирования внешних портов ввода-вывода;

- должны использоваться сертифицированные средства аутентификации;
- должно быть обеспечено автоматическое блокирование рабочего стола при простое АРМ более 5 минут;
- на АРМ должна обеспечиваться регистрация событий (вход/выход в систему, вывод информации на печать или отчуждаемые носители информации, подключение внешних устройств, смена пароля, создание и удаление учетных записей пользователей, изменение прав доступа);
- АРМ должны быть расположены в локальной сети, для разделения сетей должны использоваться межсетевые экраны, сертифицированные по требованиям безопасности информации Федеральной службой по техническому и экспортному контролю (ФСТЭК России) и соответствующие требованиям к межсетевым экранам по классу защиты не ниже 6;
- доступ в помещение с размещенными АРМ Пользователей должен контролироваться и осуществляться на основании утвержденного должностным лицом Исполнителя списка. Время работы должно регистрироваться в журнале.

8.2.2. Обеспечение защищенного подключения

Доступ Пользователей к подсистемам СУЭ осуществляется с помощью сертифицированного СКЗИ «Континент-АП», установленного на АРМ Пользователей, с помощью которого осуществляется подключение к серверу доступа установленному в ФК.

При организации защищенного подключения к подсистемам СУЭ все остальные сетевые подключения на АРМ Пользователя блокируются.

СКЗИ, устанавливаемые на оборудовании Исполнителя и необходимые для организации защищенного взаимодействия с Заказчиком, приобретаются, настраиваются и сопровождаются Исполнителем самостоятельно в соответствии с требованиями эксплуатационной документации к нему и законодательства Российской Федерации.

Приложение

к Регламенту предоставления доступа к
подсистемам Системы управления
эксплуатацией Федерального казначейства,
утвержденному приказом Федерального
казначейства

от _____ № _____

Заявка на выдачу сертификатов ключей аутентификации и шифрования и предоставление доступа к подсистемам СУЭ

Директору ФКУ «ЦОКР»

(ФИО)

Уважаемый(ая) *ФИО*!

(Наименование организации), действуя в рамках заключенного
Государственного контракта № _____ от _____ (в рамках гарантийных
обязательств по Государственному контракту № _____ от _____),
просит Вас во исполнение пункта ____ выдать сертификаты ключей
аутентификации и шифрования, необходимые для предоставления доступа к
подсистемам СУЭ в соответствии с Приложением к настоящему письму.

Машинный носитель информации, содержащий файлы запросов на
выпуск сертификатов, прилагается.

Руководитель

(или уполномоченное им лицо) _____

(подпись)

(ФИО)

Приложение

к Заявке на выдачу сертификатов ключей аутентификации и шифрования и предоставление доступа к подсистемам СУЭ

Наименование организации (Исполнителя):
 Реквизиты Государственного контракта Исполнителя, в рамках которого будут эксплуатироваться подсистемы СУЭ ФК:

Контактное лицо Исполнителя:
 ФИО:
 Должность:
 E-mail:
 Телефон:

Список Пользователей Исполнителя, наделенных правом доступа к подсистемам СУЭ ФК

№	ФИО	Должность	Подразделение	Адрес электронной почты в сети Интернет	Номер телефона	Период действия сертификата	Список подсетей из которых запланирован доступ	Сведения об ознакомлении с Регламентом предоставления доступа к подсистемам СУЭ ФК	Подпись	Перечень подсистем СУЭ, сетевых адресов и протоколов
1	2	3	4	5	6	7	8	9	10	11
1.										ПУПЭ: Протокол TCP:443 (https) адрес: 10.128.50.10 ПХКЭ: UCMDb (web) Протоколы: TCP:8080 TCP:8443 TCP:80 TCP:443 Адрес: 10.128.50.21 Asset Manager (web) Протокол:

[illegible]