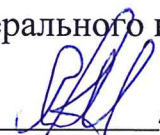


УТВЕРЖДАЮ

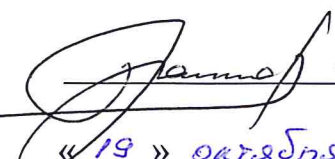
Заместитель руководителя
Федерального казначейства


_____/А.С. Албычев/
« 22 » октября 2018 г.

**РЕГЛАМЕНТ
ПРЕДОСТАВЛЕНИЯ УДАЛЕННОГО ДОСТУПА
К ИНФОРМАЦИОННЫМ РЕСУРСАМ
ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА**

СОГЛАСОВАНО

Начальник Управления
режима секретности
и безопасности информации


_____/В.С. Бражко/
« 19 » октября 2018 г.

Москва, 2018

Содержание

1. Сокращения и определения	3
2. Общие положения	6
3. Перечень работ, осуществляемых в режиме удаленного доступа	7
4. Организация удаленного доступа	8
4.1 Предварительные мероприятия	10
4.2 Подготовка и выполнение запроса на выполнение работ	10
4.3 Проведение работ.	11
4.4 Окончание работ.	12
5. Обеспечение безопасности информации при удаленном доступе Исполнителей работ к ИС ОрФК.	14
5.1 Организационные меры безопасности	14
5.2 Технические меры безопасности	15
Приложение № 1	19
Приложение № 2	22
Приложение № 3	24
Приложение № 4	25

1. Сокращения и определения

В целях настоящего Регламента используются следующие сокращения и определения:

1.1. Сокращения

АРМ	Автоматизированное рабочее место
АПКШ	Аппаратно-программный комплекс шифрования
АС ФК	Автоматизированная система Федерального казначейства
ВТС	Ведомственная транспортная сеть
ДУБП	Другой участник бюджетного процесса
ИБ	Информационная безопасность
ИС ОрФК	Информационные системы Федерального казначейства, государственные информационные системы, оператором которых является Федеральное казначейство, информационные системы ФКУ «ЦОКР».
ЗКВС	Защищенный контур вычислительной сети
ЛВС	Локальная вычислительная сеть
МНИ	Машинный носитель информации
НСД	Несанкционированный доступ
ОрФК	Центральный аппарат Федерального казначейства, территориальный орган Федерального казначейства, ФКУ «ЦОКР»
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СКЗИ	Средство криптографической защиты информации
СКУД	Система контроля удаленного доступа
СУЭ	Система управления эксплуатацией
ТОФК	Территориальный орган Федерального казначейства
ФК	Федеральное казначейство
ФКУ «ЦОКР»	Федеральное казенное учреждение «Центр по обеспечению деятельности Казначейства России»

ФСТЭК	Федеральная служба по техническому и экспортному контролю
ЦАФК	Центральный аппарат Федерального казначейства

1.2. Определения:

Исполнитель	Юридическое лицо, заключившее с ФКУ «ЦОКР» государственный контракт на выполнение работ по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации ИС ОрФК
Исполнитель работ	Сотрудник Исполнителя, непосредственно выполняющий работы, связанные с удаленным доступом к ИС ОрФК
Эксплуатирующее подразделение	Подразделение, ответственное за эксплуатацию информационной системы (подсистемы), к которой осуществляется удаленный доступ
Заказчик	Юридическое лицо, являющееся заказчиком работ по заключенному государственному контракту
Администратор ИБ	Сотрудник, ответственный за обеспечение и контроль доступа к ИС ОрФК Исполнителей работ
Удаленный доступ	Доступ Исполнителя работ к ИС ОрФК, осуществляемый из внешней сети, не контролируемой Заказчиком
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 ФКУ «ЦОКР» 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 работ 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)
Сетевой компонент	Объект сетевой инфраструктуры (рабочая станция, сервер, маршрутизатор и др.)
Сервер доступа ЗКВС	Программное обеспечение, установленное на АПКШ и предназначенное для авторизации сессий удаленного доступа через сеть ВТС
Сервер доступа сегмента «Интернет»	Программное обеспечение, установленное АПКШ и предназначенное для авторизации сессий удаленного доступа через сеть «Интернет».

2 Общие положения

Реализация удаленного доступа сотрудников Исполнителя к ИС ОрФК позволяет значительно повысить оперативность и качество выполнения работ, связанных с сопровождением и обслуживанием ИС ОрФК.

Использование СКУД обеспечивает безопасный удаленный доступ к ИС ОрФК в соответствии с требованиями законодательства Российской Федерации и нормативных правовых актов органов государственной власти, регулирующих отношения в области защиты информации, не содержащей сведений, составляющих государственную тайну.

Исполнитель работ осуществляет удаленный доступ к ИС ОрФК только на основании и с соблюдением всех условий действующего государственного контракта, предусматривающего оказание услуг/проведение работ по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации ИС ОрФК.

Настоящий регламент определяет порядок предоставления удаленного доступа для Исполнителей работ и соответствующие требования по обеспечению ИБ.

Требования о выполнении условий настоящего Регламента включаются в тексты государственных контрактов, предусматривающих удаленный доступ к ИС ОрФК.

Порядок обмена материалами, содержащими сведения конфиденциального характера, указан в государственном контракте, в рамках которого предоставляется удаленный доступ к ИС ОрФК.

Использование средств СКУД должно обеспечивать возможность контроля, мониторинга и записи действий Исполнителей работ. Примерная схема обеспечения удаленного доступа Исполнителей работ к ИС ОрФК в ТОФК приводится в Приложении № 1.

Все Исполнители работ и сотрудники ОрФК, участвующие в процессах организации, предоставления и контроля предоставления доступа, обязаны ознакомиться с настоящим Регламентом под подпись.

3 Перечень работ, осуществляемых в режиме удаленного доступа

В режиме удаленного доступа могут выполняться следующие работы по сопровождению и обслуживанию ИС ОрФК:

- мониторинг работы общего и прикладного ПО ИС ОрФК;
- проведение плановых работ, предусмотренных технологическими регламентами сопровождения ИС ОрФК;
- проведение работ по восстановлению работоспособности ИС ОрФК после отказов и сбоев СВТ;
- внесение (согласованных с Заказчиком, или представителем Заказчика в месте проведения работ) изменений в настройки ПО и в конфигурации технических средств;
- другие работы, обеспечивающие устойчивую работу ИС ОрФК.

4 Организация удаленного доступа

Необходимым условием предоставления удаленного доступа к ИС ОрФК является согласование доступа Исполнителей работ. Согласование доступа осуществляется до начала проведения работ и проводится для всех видов работ персонально для каждого Исполнителя работ.

До начала работ, предусматривающих удаленный доступ, Исполнитель направляет Заказчику на согласование Заявку на выдачу сертификатов ключей аутентификации и шифрования, необходимых для предоставления удаленного доступа, содержащих сведения об Исполнителях работ, сроках предоставления доступа, контактные данные ответственного лица Исполнителя для решения вопросов взаимодействия и другие данные по форме, представленной в Приложении № 2 настоящего Регламента, файлы запросов на выпуск сертификатов, записанные на МНИ, на всех сотрудников, указанных в Заявке (процедура генерации запроса на получение сертификата описана в документации к СКЗИ «Континент-АП») без закрытого ключа (далее – Заявка). При генерации запроса на получение сертификата необходимо заполнять поля в соответствии с требованиями, указанными в Таблице 1.

Таблица 1

Поле	Содержание	Пример
Имя сотрудника	[реквизиты государственного контракта] ФИО сотрудника полностью	[ФКУ0635] Иванов Иван Иванович
Описание	<Краткое наименование организации Исполнителя>_<первая буква имени сотрудника>_<фамилия сотрудника> (заполняется латиницей)	PPO_I_Ivanov
Организация	Наименование исполнителя	ООО ППО
Подразделение	Наименование организации субподрядчика (при заявке за сотрудника организации субподрядчика). При заявке на сотрудника Исполнителя – аналогично полю «Организация».	ООО ОПО

Регион	Город расположения Исполнителя	Москва
Город	Город расположения Исполнителя	Москва
Страна	RU	RU
E-Mail	Адрес электронной почты сотрудника Исполнителя в сети Интернет	Ivanov@ppo.ru

Срок действия сертификата ключа аутентификации и шифрования определяется условиями государственного контракта, в рамках исполнения которого удаленный доступ запрашивается.

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 рамках исполнения которого удаленный доступ запрашивается), Исполнитель направляет в адрес Заказчика Заявку в соответствии с требованиями настоящего раздела Регламента.

Срок рассмотрения Заявки подразделениями ЦА ФК и ФКУ «ЦОКР» не должен превышать 3 рабочих дней.

Внесение изменений в перечень Исполнителей работ осуществляется путем направления Заказчику новой Заявки в порядке аналогичном изложенному выше.

В случае необходимости заблокировать/отозвать сертификат сотрудника не связанной с компрометацией закрытого ключа аутентификации и шифрования, например, при прекращении трудовых обязательств сотрудника, Исполнитель должен направить Заказчику письмо с объяснением причин блокировки.

Процесс обеспечения удаленного доступа включает в себя следующие этапы:

4.1 Предварительные мероприятия

После согласования Заявки список Исполнителей работ передаётся Администратору ИБ ФКУ «ЦОКР» для формирования сертификатов ключей аутентификации и шифрования для указанных в Заявке Исполнителей работ на основе запросов на получение сертификатов, предоставленных Исполнителем.

В срок не позднее 7 рабочих дней после согласования Заявки Заказчик обязан направить Исполнителю работ личный и корневой сертификаты на адрес электронной почты, указанный в файле запроса на выпуск сертификата, либо официальным письмом отказать в предоставлении удаленного доступа с указанием причин отказа. Выпущенные сертификаты ключей аутентификации и шифрования размещаются Администратором ИБ ФКУ «ЦОКР» на сервере ЦА ФК (каталог ftp://fap.fsfk.local/remote_access/certificate).

4.2 Подготовка и выполнение запроса на выполнение работ

4.2.1. При возникновении необходимости проведения работ по сопровождению или обслуживанию ИС ОрФК в режиме удаленного доступа Эксплуатирующее подразделение (отдел информационных систем в случае работ в ТОФК) создает заявку на предоставление удаленного доступа в СУЭ по форме, представленной в Приложении № 3 настоящего Регламента.

Данная заявка адресуется Администратору ИБ ТОФК (в случае удаленного доступа к ресурсам ТОФК)/ЦОКР (в случае удаленного доступа к ресурсам ЦАФК или ФКУ «ЦОКР») (либо лицу его замещающему). Администратор ИБ ТОФК /ЦОКР принимает решение о допуске Исполнителя к работам, ставит в заявке на предоставление удаленного доступа отметку о предоставлении доступа и времени начала проведения работ.

4.2.2. Администратор ИБ ТОФК/ЦОКР скачивает сертификат назначенного Исполнителя работ с указанного выше FTP-ресурса и устанавливает (или разблокирует, в случае если сертификат установлен и блокирован) сертификат ключа аутентификации, указанного в СУЭ, Исполнителя работ на Сервер доступа ВТС (или в случае неработоспособности основного канала связи Исполнителя – на Сервер доступа сегмента «Интернет»).

4.2.3 Администратор ИБ ТОФК/ЦОКР на основании данных, полученных от Эксплуатирующего подразделения, настраивает СКУД и сообщает в Эксплуатирующее подразделение информацию об IP-адресах и портах СКУД, с использованием которых возможно получить доступ к запрашиваемым информационным ресурсам.

4.2.4 Сотрудник Эксплуатирующего подразделения формирует/разблокирует (при первичном предоставлении доступа Исполнителю работ) учетные записи назначенных на инцидент Исполнителей работ на каждом сетевом компоненте, к которому будет осуществляться удаленный доступ. **Учетная запись должна соответствовать данным, указанным в заявке на предоставление удаленного доступа в СУЭ.**

4.2.5 Сотрудник Эксплуатирующего подразделения высылает (при первичном предоставлении доступа Исполнителю работ) Исполнителю работ временный пароль электронной почтой, а также данные о СКУД, полученные от Администратора ИБ ТОФК/ЦОКР.

Внимание: После первого входа в систему Исполнитель работ обязан сменить временный пароль на постоянный.

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.

4.3 Проведение работ.

Удаленный доступ и проведение работ осуществляется только Исполнителями работ, указанными в заявке на предоставление удаленного доступа в СУЭ.

Администратор ИБ ТОФК/ЦОКР имеет право с использованием соответствующего функционала СКУД подключаться и контролировать сессию Исполнителя работ в режиме реального времени и прервать ее в случае выявления нарушений требований обеспечения ИБ с последующим оформлением соответствующего акта (Приложение № 4 к настоящему Регламенту).

В случае отсутствия пользовательской активности на сессию Исполнителя работ может накладываться ограничение по времени равное 15 минутам, по истечении которых происходит отключение сеанса без его завершения.

4.4 Окончание работ.

Исполнитель работ должен закрыть все сессии, открытые при осуществлении удаленного доступа. Администратор ИБ ТОФК/ЦОКР блокирует сертификат ключа аутентификации и шифрования на Сервере доступа ВТС ТОФК/ЦАФК (или в случае неработоспособности основного канала связи Исполнителя с ТОФК/ЦАФК – на Сервере доступа «Интернет» ТОФК/ЦАФК).

Внимание: При завершении государственного контракта, в рамках которого осуществлялся удаленный доступ Исполнителей работ, Администраторы ИБ ТОФК/ЦОКР обязаны незамедлительно удалить установленные на Серверах доступа сертификаты ключей аутентификации и шифрования соответствующих Исполнителей работ.

Схема алгоритма предоставления удаленного доступа к ИС ОрФК представлена на рисунке 1.

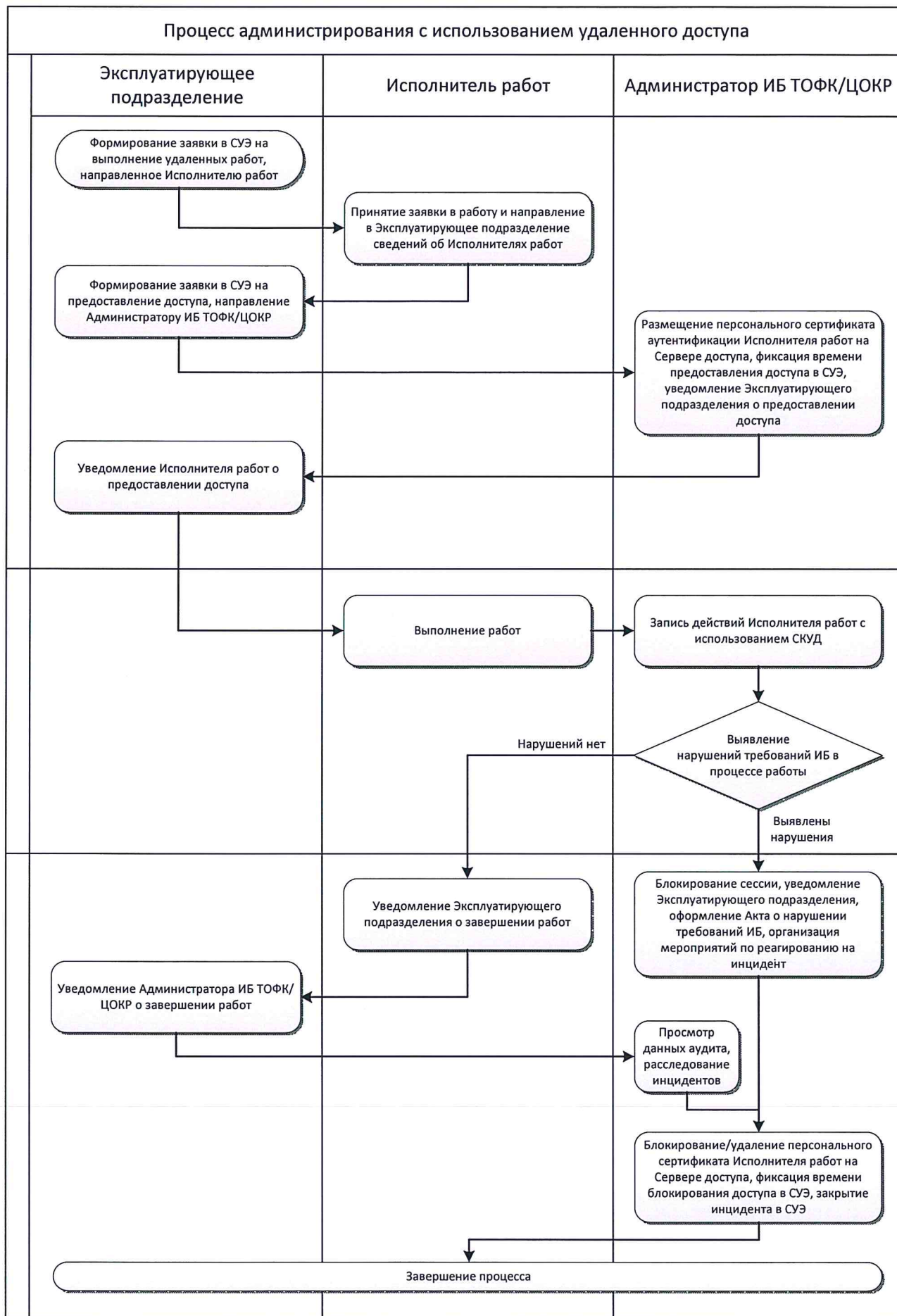


Рисунок 1 **Схема алгоритма предоставления удаленного доступа**

5 Обеспечение безопасности информации при удаленном доступе Исполнителей работ к ИС ОрФК.

Обеспечение безопасности информации при удаленном доступе Исполнителей работ к ИС ОрФК включает следующие меры безопасности:

- организационные;
- технические;
- контроль за исполнением работ.

Исполнитель подтверждает выполнение мер по защите информации, изложенных в настоящем регламенте, и обязуется выполнять их весь срок действия государственного контракта, в соответствии с которым предоставляется доступ. Информация об этом направляется официальным письмом в адрес Заказчика до начала работ, предусматривающих удаленный доступ.

5.1 Организационные меры безопасности

При удаленном доступе Исполнителей работ должны выполняться следующие требования по организации работ:

- обязательным условием для выполнения работ, предусматривающих удаленный доступ к ИС ОрФК, является наличие в государственном контракте, в соответствии с которым предоставляется доступ, пунктов, предусматривающих обязанности и ответственность Исполнителя за обеспечение конфиденциальности и выполнение требований по безопасности информации, предусмотренных законодательством Российской Федерации, нормативными правовыми актами органов государственной власти, организационно-распорядительными документами Федерального казначейства, регулирующими отношения в области защиты информации;

- данные СКУД, полученные в результате мониторинга сессий Исполнителей работ, являются основанием для рассмотрения инцидентов информационной безопасности/проверки качества выполненных Исполнителем работ, и не могут использоваться без согласования с Заказчиком;

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

- не допускается работа нескольких Исполнителей работ под одной учетной записью;

- в случае компрометации закрытого ключа аутентификации и шифрования Исполнитель обязан незамедлительно уведомить Администратора ИБ ТОФК/ЦОКР средствами электронной почты, отправив письмо на почтовый ящик *rud@roskazna.ru*, для оперативной блокировки сессии и удаления сертификатов с Серверов доступа. Для восстановления удаленного доступа Исполнитель должен направить повторную заявку в соответствии с пунктом 4 настоящего Регламента;

5.2 Технические меры безопасности

Технические меры должны включать соблюдение требований обеспечения безопасности информации:

- при работе на АРМ Исполнителя работ;
- при подключении к сети ОрФК по защищенным каналам доступа;
- в процессе выполнения всех видов работ, с использованием удаленного доступа.

5.2.1 Обеспечение безопасности на АРМ Исполнителя работ

Для АРМ Исполнителя работ должны выполняться следующие требования:

- должны применяться сертифицированные средства защиты информации и средства криптографической защиты информации;

- должны применяться сертифицированные средства антивирусной защиты;

- должны применяться средства блокирования внешних портов ввода-вывода;

- должны быть установлены клиенты удаленного доступа;

- 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, изолированной от других сетей, или для разделения сетей должны использоваться межсетевые экраны, сертифицированных по требованиям безопасности информации в соответствии с руководящим документом ФСТЭК «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» не ниже 4 класса;

- доступ в помещение с размещенными АРМ Исполнителей работ должен контролироваться и осуществляться на основании утвержденного должностным лицом Исполнителя списка. Время работы должно регистрироваться в журнале.

5.2.2 Обеспечение защищенного подключения

Удаленное подключение к сети ОрФК осуществляется с помощью сертифицированных средств криптографической защиты информации. На АРМ Исполнителей работ устанавливается клиентское ПО удаленного доступа, с помощью которого осуществляется подключение к Серверу доступа ЗКВС или Серверу доступа сегмента «Интернет», установленному в ОрФК.

При организации защищенного подключения к ИС ОрФК все остальные сетевые подключения на АРМ Исполнителя работ блокируются.

Средства криптографической защиты информации, 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 ним и законодательства Российской Федерации.

С целью обеспечения аутентификации Исполнителей работ в ЦАФК установлен Сервер доступа, корневым сертификатом ключа которого используется

для обеспечения удаленного доступа на соответствующих серверах доступа ЗКВС или серверах доступа сегмента «Интернет», установленных в ОрФК. При этом:

- Исполнитель работ получает в установленном в пункте 4.1 настоящего Регламента порядке личный и корневой сертификаты ключа аутентификации и шифрования;

- Корневой сертификат и сертификаты ключей аутентификации и шифрования Исполнителей работ размещаются Администратором ИБ ЦОКР на FTP-сервере в ЗКВС ЦАФК;

- установка сертификатов ключей аутентификации и шифрования Исполнителей работ осуществляется только на серверы доступа ЗКВС, включенные в ВТС или, при отсутствии возможности подключения через сеть ВТС, на серверы доступа сегмента «Интернет» (далее – Серверы доступа ОрФК). При этом обеспечивается возможность контролировать на Серверах доступа ОрФК адрес источника доступа и, в случае нелегитимного доступа (например, при маршрутизации Исполнителем несанкционированного трафика из сети Интернет), прерывать соответствующую сессию, а также не допускать Исполнителя работ при несоответствии его идентификационных данных на Серверах доступа ОрФК и названия учетной записи на сетевом компоненте ОрФК;

- для одного Исполнителя работ (в рамках одного государственного контракта) централизованно выдается один сертификат ключа аутентификации и шифрования.

5.2.3 Меры безопасности информации

При удаленном доступе Исполнителей работ должны выполняться следующие меры информационной безопасности:

- должно обеспечиваться исключение возможности удаленного доступа в обход СКУД;

– должен блокироваться доступ с ИС ОрФК к локальным ресурсам АРМ Исполнителя работ (к терминальному серверу ОрФК запрещается монтирование флеш-носителей, жестких дисков и прочих локальных ресурсов, подключенных к АРМ Исполнителя работ);

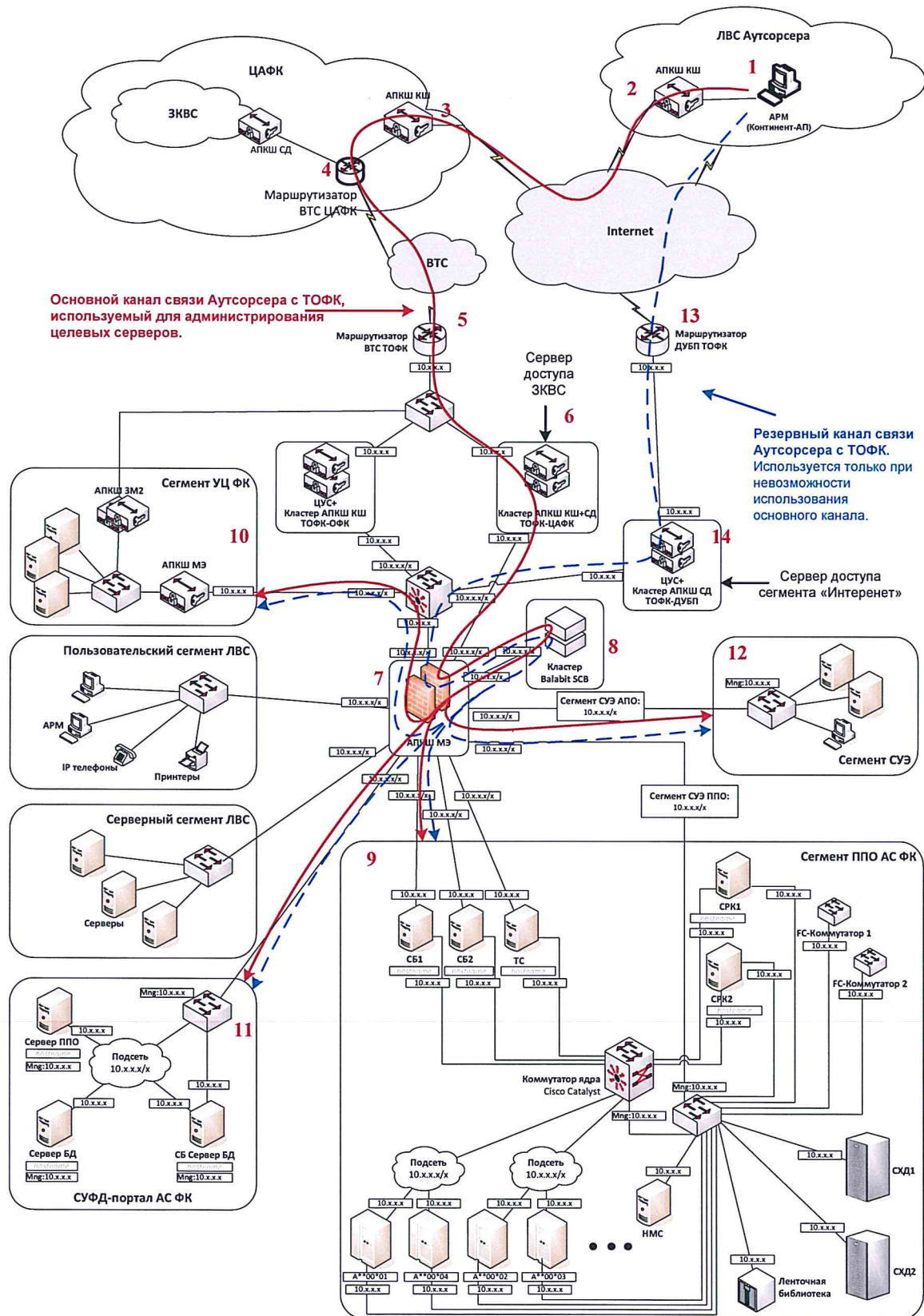
– Администратор ИБ ТОФК/ЦОКР имеет право на разблокировку, контроль и блокировку сессий Исполнителей работ, используя функциональные возможности СКУД;

– записи в журналах СКУД должны храниться в течение 1 месяца со дня их регистрации и не менее 6 месяцев при их архивном хранении.

Приложение № 1

к Регламенту предоставления удаленного доступа к информационным ресурсам Федерального казначейства

Примерная схема обеспечения удаленного доступа Исполнителей работ к информационным системам Федерального казначейства в ТОФК



**Описание примерной схемы обеспечения удаленного доступа
Исполнителей работ к информационным системам Федерального
казначейства в ТОФК**

1. Использование основного канала связи.

1. В целях организации защищенного канала связи Исполнителя и Заказчика, в сети Исполнителя и в сети ЦАФК установлены АПКШ КШ (2 и 3 соответственно).

2. Исполнитель работ, используя программное обеспечение «Континент - АП» с АРМ пользователя (1) через АПКШ КШ Исполнителя (2), АПКШ КШ Заказчика (3), маршрутизатор ВТС ЦАФК (4), ВТС, маршрутизатор ВТС ТОФК (5) аутентифицируется и авторизуется на сервере доступа (АПКШ КШ+СД ТОФК - ЦАФК) (6).

3. После успешной авторизации на Сервере доступа ЗКВС (6), Исполнитель работ, через межсетевой экран АПКШ МЭ (7) маршрутизируется на систему контроля удаленного доступа «Balabit SCB» (8).

4. После установление соединения с «Balabit SCB» (8), Исполнитель работ, в соответствии с правилами, заданными на «Balabit SCB», маршрутизируется на стандартные RDP (SSH, Telnet) порты целевых серверов (9, 10, 11, 12) через межсетевой экран АПКШ МЭ (7).

2. Использование резервного канала связи.¹

1. Исполнитель работ, используя программное обеспечение «Континент - АП» с АРМ пользователя (1) через сеть «Интернет», маршрутизатор ДУБП ТОФК (13) аутентифицируется и авторизуется на сервере доступа сегмента «Интернет» (АПКШ СДТОФК - ДУБП) (14).

2. После успешной авторизации на Сервере доступа сегмента «Интернет» (14), Исполнитель работ, через межсетевой экран АПКШ МЭ (7) маршрутизируется на систему контроля удаленного доступа «Balabit SCB» (8).

¹ Допускается только при невозможности использования основного канала связи Исполнителя с Заказчиком.

3. После установления соединения с «Balabit SCB» (8), Исполнитель работ, в соответствии с правилами, заданными на «Balabit SCB», маршрутизируется на стандартные RDP (SSH, Telnet) порты целевых серверов (9, 10, 11, 12) через межсетевой экран АПКШ МЭ (7).

Приложение № 2

к Регламенту предоставления удаленного доступа к
информационным ресурсам Федерального казначейства

Заявка на выдачу сертификатов ключей аутентификации и шифрования, необходимых для предоставления удаленного доступа

Ответственному лицу

Заказчика

(ФИО)

Уважаемый(ая) ФИО!

(Наименование организации), действуя в рамках заключенного государственного контракта №_____ от _____, просит Вас во исполнение пункта __, выдать сертификаты ключей аутентификации и шифрования, необходимых для предоставления удаленного доступа, исполнителям работ, наделенных правом удаленного доступа к информационным ресурсам Федерального казначейства, в соответствии с Приложением к настоящему письму.

Руководитель

(или уполномоченное им лицо) _____

(подпись)

_____ (ФИО)

Исполнитель:

(ФИО)

(адрес эл. почты), (телефон)

Список исполнителей работ наделенных правом удаленного доступа к информационным ресурсам
Федерального казначейства

№	ФИО	Должность, подразделение	Адрес электронной почты в сети Интернет	Номер телефона	Период действия сертификата	Список подсетей из которых запланирован удаленный доступ	Сведения об ознакомлении с Регламентом предоставления удаленного доступа к ИР ФК	Подпись
1	2	3	4	5	6	7	8	9
1.								
2.								

Приложение № 3

к Регламенту предоставления удаленного доступа к информационным ресурсам Федеральным казначейства

Заявка на предоставление удаленного доступа к информационным ресурсам ОрФК

[illegible]

Приложение № 4

к Регламенту предоставления удаленного доступа к
информационным ресурсам Федерального казначейства

ФОРМА АКТА ПРЕРЫВАНИЯ СЕССИИ УДАЛЕННОГО ДОСТУПА

АКТ ____

ПРЕРЫВАНИЯ СЕССИИ УДАЛЕННОГО ДОСТУПА

г. _____

« ____ » _____ 20 ____ г.

Мы, нижеподписавшиеся:

Администратор ИБ _____,

сотрудник Эксплуатирующего подразделения _____,

составили настоящий акт о том, что по причине выявления нарушений
требований информационной безопасности были прерваны следующие
сессии удаленного доступа:

№ п/п	ФИО Исполнителя работ	Дата и время начала сессии	Дата и время прерывания сессии	Выявленные нарушения

Администратор ИБ

(фамилия)

(подпись)

Сотрудник
Эксплуатирующего
подразделения

(фамилия)

(подпись)