Регламент по подключению к защищенному криптографическому соединению класса КС3

Версия 1.1

на 18 листах

Москва 2021

Управление документом

Версия	Дата	Автор	Комментарии
1.1	01.02.2021	Александров И.В.	Разработка документа

Содержание

1 Термины и определения

Термин	Определение
ЕБС или Единая биометрическая система	Единая информационная система персональных данных, обеспечивающая обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
Интегратор	Уполномоченная Оператором криптосети организация на выполнение интеграционных работ по подключению Участника БВ к криптосети
Криптосеть	Защищенное криптографическое соединение класса КС3 на технологическом участке взаимодействия с Единой биометрической системой
ЛК ЕБС	Личный кабинет организации, расположенный на портале https://bio.rt.ru
Оператор криптосети	Публичное акционерное общество «Ростелеком» (далее – ПАО «Ростелеком»)
Портал ЕБС	Портал Единой биометрической системы, расположенный по адресу https://bio.rt.ru
УЗ	Учётная запись
Участник БВ	Участник биометрического взаимодействия (Юридическое лицо, использующее криптосеть)
ЦКиЗ	Центр кибербезопасности и защиты ПАО «Ростелеком»

2 Введение

Настоящий документ содержит описание процедуры подключения Участника биометрического взаимодействия к информационной инфраструктуре Оператора криптосети с применением СКЗИ класса КС3 на технологическом участке взаимодействия с Единой биометрической системой.

3 Нормативные и полезные ссылки

При разработке настоящего регламента были использованы нормы, требования и рекомендации, приведённые в следующих законодательных, нормативных правовых и иных актах и документах:

1. Федеральный закон РФ от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»;
2. Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
3. Федеральный закон РФ от 07.07.2003 № 126-ФЗ «О связи»;
4. Приказ ЦБ РФ «О перечне угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 статьи 141 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в единой биометрической системе»;
5. Методические рекомендации по работе с ЕБС;
6. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
7. Приказ ФСБ РФ от 9.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
8. Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных».

4 Роли участников регламентных процедур

Перечень ролей организаций, участвующих в процессе подключения, указан в Таблице 1.

Таблица 1 – Роли регламентных процессов

№	Роль	Описание
1	Оператор криптосети	Оператор защищенного криптографического соединения класса КС3. Выполняет операторские функции криптосети и обеспечивает функционирование криптосети
3	Участник БВ	Участник биометрического взаимодействия, использующий криптосеть
4	Интегратор	Уполномоченный Оператором криптосети интегратор, выполняющий работы по подключению Участника БВ к криптосети
5	ЦКиЗ	Центр кибербезопасности и защиты ПАО «Ростелеком», выполняющий работы по настройке и технической поддержке защищенного соединения при осуществлении доступа к информационной инфраструктуре Оператора криптосети с применением СКЗИ класса КС3 на технологическом участке взаимодействия с ЕБС

5 Общий порядок предоставления доступа к криптосети

Для получения доступа к криптосети, Участнику БВ[1] необходимо выполнить следующие шаги:

1. Заключить соглашение с Оператором криптосети;
2. Заключить договор с уполномоченным Интегратором на выполнение работ по подключению к криптосети;
3. Организовать защищенное криптографическими средствами класса КС3 соединение до инфраструктуры Оператора криптосети (в соответствии с настоящим регламентом).

5.1. Подача заявки на подключение

По вопросам стоимости и условиям подключения к криптосети, Участник БВ направляет заявку в свободной форме с корпоративного адреса организации на адрес sale@bio.rt.ru.

5.2. Акцепт оферты

1. Участник БВ авторизуется через ЕСИА на портале ЕБС bio.rt.ru нажав на ссылку «Профиль организации» и отправляет запрос на получение доступа к Личному кабинету организации на портале bio.rt.ru (далее – ЛК).

Внимание! *Профиль пользователя в ЕСИА должен быть привязан к профилю организации (Участника БВ) в ЕСИА.*

2. Оператор криптосети в срок не более 2 рабочих дней, предоставляет доступ к ЛК.

3. После получения доступа, Участник БВ в ЛК организации принимает соглашение на предоставление услуг (акцепт оферты) по подключению к криптосети (Публичная оферта для подключения к криптографической сети).

4. Оператор криптосети, в срок не более 2-х рабочих дней, подтверждает акцепт оферты. Акцептованная оферта размещается в ЛК организации.

Внимание! *На текущем моменте между Участником БВ и выбранным уполномоченным Интегратором должен быть заключен договор на выполнение работ по подключению к криптосети.*

Дальнейшие работы по подключению Участника БВ к криптосети выполняются Интегратором.

[1] Участник БВ должен иметь в ЕСИА учетную запись юридического лица

Выполнение работ по регламентным процедурам производится ЦКиЗ по запросу, номер которого сообщается заявителю по электронной почте после регистрации в системе контроля и первичной обработки запроса уполномоченным сотрудником.

5.3. Организация защищенного криптографическими средствами класса КС3 соединения

Предусловия процесса

- Участнику БВ проинсталлировано Интегратором оборудование криптографической защиты информации класса КС3 для организации защищенного соединения при осуществлении доступа к информационной инфраструктуре Оператора криптосети с применением СКЗИ класса КС3 на технологическом участке взаимодействия с ЕБС (в соответствии с приказом [6] и [7]).

Шаги процесса «Организация защищенного криптографическими средствами класса КС3 соединения»

Шаги процесса представлены в Таблице 3.

Условия по организации защищенного криптографическими средствами класса КС3 соединения до инфраструктуры Оператора криптосети указаны в Публичной оферте для подключения к криптографической сети.

Организация защищенного криптографическими средствами класса КС3 соединения до инфраструктуры Оператора криптосети реализуется отдельно выделенными для этого криптографическими средствами защиты информации класса КС3 (АПКШ «Континент») с действующим сертификатом соответствия ФСБ России (Приложение № 1, № 2 настоящего Регламента).

Технические параметры подключения криптографических средств защиты информации класса КС3 указаны в Приложении № 2 настоящего Регламента.

Процесс передачи ключевой информации

1. Представитель Интегратора лично приходит в Центр кибербезопасности и защиты (ЦКиЗ) ПАО «Ростелеком» с удостоверяющим документом и Доверенностью на получение ключевой информации (Приложение № 3 к настоящему Регламенту).

Адрес ЦКиЗ – 127018, Российская Федерация, г. Москва, ул. Сущевский вал, д. 26.

2. Сотрудник ЦКиЗ сверяет данные удостоверяющего документа с данными Представителя Интегратора, указанными в Доверенности на получение ключевой

информации, записывает ключевые файлы и файлы конфигурации на носитель, делает соответствующую пометку в Журнале поэкземплярного учета СКЗИ и передает носитель Представителю Интегратора вместе с сопроводительным письмом, либо Актом приема-передачи. В сопроводительном письме (Акте приема-передачи) должно быть указано: кто принял СКЗИ, в каком количестве, учетные номера изделий или документов, назначение и порядок использования высылаемого отправления.

3. Носитель с криптоключами должен быть помещен в прочную упаковку, исключающую возможность физического повреждения носителя. Сотрудник ЦКиЗ указывает на упаковке в качестве получателя Ответственного со стороны Интегратора, указанного в заявке на организацию криптоканала (Приложение № 1 к настоящему Регламенту), для которого эта упаковка предназначена, и ставит пометку «Лично». Упаковка должна иметь средства контроля вскрытия (печати, пломбы или иные), чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и средств контроля вскрытия. Ответственность за безопасность во время транспортировки несет представитель Интегратора.

4. Не более чем через 30 дней с момента передачи носителя, Интегратор должен направить Оператору криптосети Акт об уничтожении ключевого носителя.

Акт об уничтожении ключевого носителя передается Оператору криптосети в 1 (Одном) экземпляре посредством ЭДО или нарочным образом с сопроводительным письмом. Получатель – Орган криптографической защиты ПАО «Ростелеком».

Таблица 3 – Организация защищенного криптографическими средствами класса КС3 соединения до инфраструктуры Оператора криптосети

№	Шаг	Входные данные	Выходные данные	Срок испол-нения	Ответствен-ный исполнитель
1	Заявка на подключение к криптосети	Заполненная заявка (Приложение № 1 к настоящему Регламенту) отправлена на адрес **otib@bio.rt.ru**	Зарегистриро-ванный номер запроса	0,5 р.д.	Интегратор
2	Проверка входных данных заявки	Запрос на подключение	Успешное подключение / Отказ в подключении	4 р.д.	ЦКиЗ
3	Выполнить завершающие действия по запросу: – Решить запрос; – Уведомить Интегратора о решении.	Уведомление Интегратора об успешном подключении к криптосети	Сообщение по электронной почте в адрес Интегратора о решении запроса	0,5 р.д.	ЦКиЗ

№	Шаг	Входные данные	Выходные данные	Срок испол-нения	Ответствен-ный исполнитель
Максимальное время исполнения регламентной процедуры: 5 рабочих дня с момента получения полной информации по запросу при соблюдении всеми участниками временных границ своих операций.					

Внимание! *В случае отсутствия в течение 3 рабочих дней ответа от Интегратора на запрос ЦКиЗ и/или на уведомление о решении запроса, автоматически инициируется процесс Принудительного закрытия запроса.*

6 Приложение № 1. Форма заявки на организацию защищенного криптографическими средствами класса КС3 соединения

Форма заявки на организацию защищенного криптографическими средствами класса КС3 соединения

Тип заявки		*(первичная регистрация / изменение параметров[2])*
Данные об Участнике взаимодействия		
1	Полное наименование Участника БВ	*(обязательно)*
2	ОГРН	*(обязательно)*
Сотрудник, ответственный за подключение		
3	ФИО	*(обязательно)*
4	Рабочий телефон	*(обязательно)*
5	Мобильный телефон	*(обязательно)*
6	Адрес электронной почты	*(обязательно)*
Сетевой инженер, ответственный за подключение		
7	ФИО	*(обязательно)*
8	Рабочий телефон	*(обязательно)*
9	Мобильный телефон	*(обязательно)*
10	Адрес электронной почты	*(обязательно)*
Лицо, ответственное за информационную безопасность		
11	ФИО	*(обязательно)*
12	Рабочий телефон	*(обязательно)*
13	Мобильный телефон	*(обязательно)*
14	Адрес электронной почты	*(обязательно)*
Сотрудник Интегратора, ответственный за подключение		
15	ФИО	*(обязательно)*
16	Рабочий телефон	*(обязательно)*
17	Мобильный телефон	*(обязательно)*
18	Адрес электронной почты	*(обязательно)*

[2] При изменении параметров в заявке, указываются только изменяемые данные.

Объект подключения		
19	Адрес местонахождения	*(обязательно)*
20	Этаж	*(обязательно)*
21	Помещение	*(обязательно)*
22	Используемое криптооборудование	*(обязательно)*
Данные криптошлюза		
23	Лицензионный номер	*(обязательно)*
24	Заводской номер	*(обязательно)*
25	Идентификатор	*(обязательно)*
26	Строка инициализации	*(обязательно)*
Данные резервного криптошлюза *(заполнять в случае подключения кластера горячего резервирования)*		
27	Лицензионный номер	*(обязательно)*
28	Заводской номер	*(обязательно)*
29	Идентификатор	*(обязательно)*
30	Строка инициализации	*(обязательно)*
IP адреса в сети Участника БВ[3]		
31	ip/mask ext	*(обязательно заполнить и адресацию, и имя целевого интерфейса)*
32	ip/mask int	*(обязательно заполнить и адресацию, и имя целевого интерфейса)*
33	ip gw ext	*(обязательно)*
34	cluster interface	*(указать имя интерфейса в случае подключения кластера)*
35	ip fw	*(обязательно)*
36	ip gw int	*(обязательно)*
37	ip res	*(обязательно)*
* Ответственность за сбор и обработку персональных данных представителей Участника БВ в соответствии с Федеральным законом № 152-ФЗ, несет Участник БВ ** Ответственность за сбор и обработку персональных данных представителей Интегратора в соответствии с Федеральным законом № 152-ФЗ, несет Интегратор		

Должность представителя Участника БВ _____ Фамилия И. О. _____

[3] В соответствии с техническими параметрами подключения криптографических средств защиты информации класса КС3 до инфраструктуры Оператора криптосети

_____ _____

(подпись)

7 Приложение № 2. Технические параметры подключения криптографических средств защиты информации класса КС3 до инфраструктуры Оператора криптосети

Подключение кластера или одиночного криптошлюза

1. Для организации подключения кластера горячего резервирования или одиночного криптошлюза Участник БВ:

1.1. Обеспечивает выделение IP адресов в сети Участника БВ, в соответствии с типовой схемой (п. 1.9) и таблицей:

№	IP адрес/маска	Назначение
1	ip/mask ext	Активный адрес внешних интерфейсов. Может быть как из частного, так и из публичного адресного пространства
2	ip/mask int	Активный адрес внутренних интерфейсов. Ip ext и ip int обязательно должны принадлежать разным подсетям.
3	ip gw ext	Адрес шлюза по умолчанию в сети, в которую включаются внешние интерфейсы.
4	ip fw	Публичный транслируемый адрес, через который осуществляется доступ к внешнему адресу (п. 1). Указывается в случае использования частных адресов на внешних интерфейсах.
5	ip gw int	Адрес шлюза для доступа к внутренним ресурсам Участника БВ. Указывается в случае нахождения ресурсов Участника БВ и внутренних интерфейсов (п. 2) в разных сетях.
6	ip res	Адрес ресурса Участника БВ, либо адрес трансляции, с которого идут обращения через защищенный канал

1.2. Обеспечивает физическое размещение Оборудования Участника БВ, в зависимости от модели оборудования:

- Для АПКШ «Континент» 3.9 IPC-10 место размером 30 x 220 x 143 мм (ВхШхГ);
- Для АПКШ «Континент» 3.9 IPC-25 место размером 45 x 275 x 155 мм (ВхШхГ);
- Для АПКШ «Континент» 3.9 IPC-50 место размером 30 x 220 x 143 мм (ВхШхГ);

- Для АПКШ «Континент» 3.9 IPC-100 одно место размером 19 дюймов Rack 1U (для установки в стойку глубиной от 480 мм и более) 45 х 437 х 417 мм (ВхШхГ);
- Для АПКШ «Континент» 3.9 IPC-500 \ IPC-500F \ IPC-600 \ IPC-800F \ IPC-1000F \ IPC-3000F одно место размером 19 дюймов Rack 1U (для установки в стойку глубиной от 480 мм и более) 45 х 445 х 490 мм (ВхШхГ).

1.3. Обеспечивает подключение оборудования максимальной потребляемой мощностью от 40 до 300 Вт (каждый, в зависимости от выбранной модели Оборудования) к сети гарантированного электропитания питания 220 В с помощью кабеля типа C13 – CEE7/7 (евровилка);

1.4. Обеспечивает возможность подключения к сетевому оборудованию Участника БВ интерфейсов криптошлюзов с использованием интерфейсов Ethernet Base T 100/1000/10G;

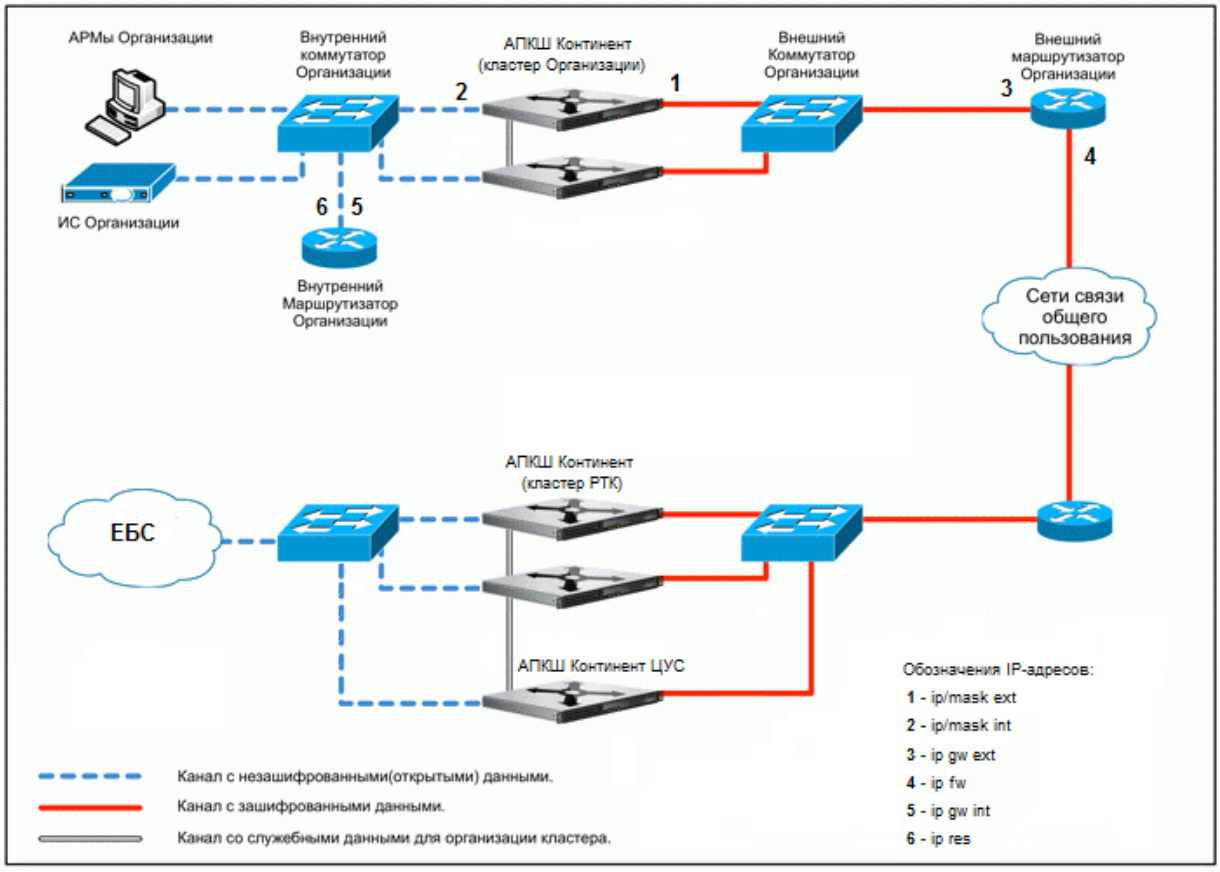
1.5. Обеспечивает связность на втором уровне модели OSI/ISO внутренних и отдельно внешних интерфейсов криптошлюзов, другими словами, размещение двух физических внутренних интерфейсов - в одном широковещательном сегменте, внешних - в другом;

1.6. Обеспечивает отсутствие логических препятствий для прохождения трафика по протоколу UDP, TCP и по портам 4431, 4444, 4445, 4446, 5100-5103, 4433, 7500, 10000-10031, 5101, 5106, 5107, 5557 между внешним адресом (ip ext) и адресами криптошлюзов криптосети.

1.7. При использовании частных адресов на внешних интерфейсах – обеспечивает статическую трансляцию адреса частного внешнего адреса (ip ext) в публичный адрес (ip fw) и трансляцию публичного адреса (ip fw) в частный внешний адрес (ip ext) по протоколам и портам согласно п. 1.6.

1.8. Обеспечивает трансляцию адресов ресурсов Участника БВ в один адрес (ip res), принадлежащий сети внутреннего адреса (ip int). В случае невозможности выделения адреса из сети внутреннего адреса - обеспечивает маршрутизацию в локальной сети Участника БВ таким образом, чтобы трафик с адреса ресурсов Участника БВ (ip res), отправляемый на серверы Оператора криптосети, направлялся на внутренний адрес (ip int).

1.9. Типовая схема подключения кластера:


АРМы Организации
Внутренний коммутатор Организации
АПКШ Континент (кластер Организации)
Внешний Коммутатор Организации
Внешний маршрутизатор Организации
ИС Организации
Внутренний Маршрутизатор Организации
Сети связи общего пользования
ЕБС
АПКШ Континент (кластер РТК)
АПКШ Континент ЦУС
Обозначения IP-адресов:
1 - ip/mask ext
2 - ip/mask int
3 - ip gw ext
4 - ip fw
5 - ip gw int
6 - ip res
Канал с незашифрованными(открытыми) данными.
Канал с зашифрованными данными.
Канал со служебными данными для организации кластера.

8 Приложение № 3. Форма Доверенности на получение ключевой информации

Заполняется на бланке организации

Д О В Е Р Е Н Н О С Т Ь

г. Москва **«___» _____ 202__ г.**

Настоящей доверенностью _____, далее – _____, адрес места нахождения: _____, ИНН _____, ОГРН _____, в лице _____, действующего на основании _____, уполномочивает сотрудника органа криптографической защиты информации

_____, паспорт: _____, выдан _____, дата выдачи _____, код подразделения _____, действовать от имени _____,

получить ключевую информацию, созданную для Участника биометрического взаимодействия – _____, расписываться в соответствующих документах для исполнения поручений, определенных настоящей доверенностью.

Настоящая доверенность выдана сроком по _____ без права передоверия полномочий по ней третьим лицам.

Подпись
Сотрудника Интегратора,
ответственного за подключение _____ подтверждаю.

Руководитель организации **И.О. Фамилия**