

Федеральное государственное унитарное предприятие

**«Главный радиочастотный центр»**

**(ФГУП «ГРЧЦ»)**

**Технические условия**

**по подключению к информационному ресурсу для передачи сетевых адресов IPv4 и IPv6**

**Москва 2025**

СОДЕРЖАНИЕ

[1 Общие сведения 3](#_Toc209079189)

[1.1 Назначение документа 3](#_Toc209079190)

[1.2 Правовые основания 5](#_Toc209079191)

[2 Порядок взаимодействия при подаче запроса на подключение к информационному ресурсу 7](#_Toc209079192)

[3 Регламент подключения 8](#_Toc209079193)

[3.1 Вариант подключения ОС к информационному ресурсу с использованием криптографического шлюза АПКШ «Континент» 8](#_Toc209079194)

[3.2 Вариант подключения ОС к информационному ресурсу с использованием абонентского пункта «Континент-АП» 10](#_Toc209079195)

[4 Данные для настройки сервиса интеграции с информационным ресурсом 12](#_Toc209079196)

[5 Заключительные положения 13](#_Toc209079197)

[5.1 Изменения и пересмотр документа 13](#_Toc209079198)

[Приложение № 1 14](#_Toc209079200)

[Приложение № 2 15](#_Toc209079201)

1. Общие сведения
	1. **Назначение документа**

Настоящие Технические условия (далее по тексту – ТУ) разработаныЦентром мониторинга и управления сетью связи общего пользования ФГУП «ГРЧЦ» в рамках выполнения задач, возложенных на Центр пунктами 2 и 3 Положения о Центре мониторинга и управления сетью связи общего пользования, утвержденного приказом Роскомнадзора от 31.07.2019 № 225 и определяют порядок подключения операторов связи (далее – ОС) и организацию защищенного канала связи к информационному ресурсу[[1]](#footnote-1) для передачи информации в соответствии с пунктом 12 приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28 февраля 2025 г. № 51 “Об утверждении порядка, сроков, состава и формата предоставления оператором связи в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, информации, позволяющей идентифицировать средства связи и пользовательское оборудование (оконечное оборудование) в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации, территории субъекта Российской Федерации или части территории субъекта Российской Федерации, в электронной форме”.

ТУ разработаны в целях обеспечения функции передачи ОС сетевых адресов пользователя, формируемых по технологии, позволяющей одновременное использование протоколов IPv4 и IPv6:

* о сетевом адресе, выделенном в формате протокола IPv4;
* о сетевом адресе, выделенном в формате протокола IPv6.

В ТУ используются следующие определения и сокращения:

**Оператор связи** - [юридическое лицо](https://ru.wikipedia.org/wiki/%D0%AE%D1%80%D0%B8%D0%B4%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%BB%D0%B8%D1%86%D0%BE) или [индивидуальный предприниматель](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D0%B4%D0%B8%D0%B2%D0%B8%D0%B4%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%BF%D1%80%D0%B5%D0%B4%D0%BF%D1%80%D0%B8%D0%BD%D0%B8%D0%BC%D0%B0%D1%82%D0%B5%D0%BB%D1%8C), оказывающие услуги связи на основании соответствующей [лицензии](https://ru.wikipedia.org/wiki/%D0%9B%D0%B8%D1%86%D0%B5%D0%BD%D0%B7%D0%B8%D1%8F);

**Значимый объект критической информационной инфраструктуры** (ЗОКИИ)- объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

**Конфиденциальность информации -** обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такуюинформацию третьим лицам без согласия ее собственника;

**Администратор информационной безопасности** (далее — Администратор ИБ) — работник (служащий), с соответствующей квалификацией, осуществляющий обеспечение устойчивой работоспособности элементов ИС и средств защиты информации.

**Ответственный за защиту информации -** работник (служащий), с соответствующей квалификацией, который обеспечивает соблюдение требований законодательства в области защиты информации, организует и контролирует применение мер защиты данных, а также взаимодействует с надзорными органами.

**Администратор СКЗИ -** работник (служащий), с соответствующей квалификацией, осуществляющий обеспечение работоспособности средств криптографической защиты информации.

**Политика информационной безопасности** - это набор правил, процедур и руководящих принципов, которые используются для защиты информационных активов от различных угроз в целях обеспечения конфиденциальности, целостности и доступности информации, а также минимизировать риски для бизнеса. Соответствие политикам безопасности определяется наличием у Оператора связи организационно-распорядительных документов по защите информации (регламент, инструкция, положение и т.д.), соответствующей инфраструктуры и/или оборудования для подключения к информационному ресурсу по защищенному каналу связи ГОСТ VPN не ниже КС3 и назначением Ответственного за защиту информации.

**Аппаратно-программный комплекс шифрования «Континент»** (далее - АПКШ «Континент», АПКШ) - [аппаратно-программный комплекс](https://ru.wikipedia.org/wiki/%D0%90%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81), позволяющий обеспечить построение защищенного соединения между инфраструктурой информационного ресурса и инфраструктурой ОС в рамках стандарта ГОСТ VPN.

**Центр управления сетью АПКШ** (далее – ЦУС) – техническое, программное или программно-техническое средство, которое входит в состав [аппаратно-программного комплекса шифрования «Континент»](https://www.google.com/search?sca_esv=ba24c2d2484ecd3d&rlz=1C1GCEU_ruRU1145RU1147&q=%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE-%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B3%D0%BE+%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%B0+%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F+%22%D0%9A%D0%BE%D0%BD%D1%82%D0%B8%D0%BD%D0%B5%D0%BD%D1%82%22&sa=X&ved=2ahUKEwiiw_qP_KuPAxUyKBAIHV1sKEoQxccNegQIIBAB&mstk=AUtExfD7s5QxXVrBFAcUqnfcX2PxN8vtH4AZlB1myPWX8JYY8xKKz_LK7wJiMMqCUaOkHwZmUl4zFaAA5fFtgEyeEP8nh9Gm-2fYH_PI_Q4E4oY8qjjmYITQGITF4TBS2Ym-VWE&csui=3), предназначенное для централизованного управления и мониторинга работы всех сетевых устройств комплекса.

**Центр мониторинга и управления сетью связи общего пользования** ФГУП «ГРЧЦ»(далее - ЦМУ ССОП ФГУП «ГРЧЦ») – центр мониторинга и управления сетью связи общего пользования в структуре ЦМУ ССОП ФГУП «ГРЧЦ», предназначенный для обеспечения организационно-технических мер, необходимых для реализации Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) полномочий, предусмотренных Федеральным законом от 7 июля 2003 г. №126-ФЗ «О связи».

**ГОСТ VPN-туннель** – стандарт построения защищенного канала связи для передачи данных в сети Интернет с использованием алгоритмов шифрования ГОСТ.

* 1. **Правовые основания**

В настоящем документе применены термины и определения в соответствии с [ГОСТ Р 50922](http://docs.cntd.ru/document/1200058320), [ГОСТ Р 53114](http://docs.cntd.ru/document/1200075565), [ГОСТ Р 59853](https://docs.cntd.ru/document/578500096), а также термины и определения, установленные законодательством Российской Федерации и национальными стандартами в области защиты информации и обеспечения информационной безопасности.

Настоящие ТУ разработаны с учетом требований:

* Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
* Федерального закона Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»;
* Федерального закона Российской Федерации от 7 июля 2003 года № 126-ФЗ «О связи»;
* Федерального закона Российской Федерации от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
* Приказа ФАПСИ от 13 июня 2001 г. № 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»;
* Приказа ФСБ России от 18.03.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»;
* Приказа ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
* Приказа ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования;
* Приказа ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации;
* Приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14 декабря 2017 г. № 249 «Об утверждении требований к способам (методам) ограничения доступа к информационным ресурсам, а также требований к размещаемой информации об ограничении доступа к информационным ресурсам»;

ТУ разработаны в связи с локально-нормативными актами (далее — ЛНА) и регламентирующими документами ЦМУ ССОП ФГУП «ГРЧЦ».

Настоящие ТУ могут развиваться другими внутренними ЛНА и организационно-распорядительными документами по защите информации (далее — ОРД), которые дополняют и уточняют его.

1. Порядок взаимодействия при подаче запроса на подключение к информационному ресурсу

ЦМУ ССОП ФГУП «ГРЧЦ» предоставляет доступ Оператору связи (далее - ОС) к API интерфейсу Dual-Stack, при условии организации защищенного канала связи ГОСТ VPN КС3.

Информационное взаимодействие ОС с ЦМУ ССОП ФГУП «ГРЧЦ» и подключение к API интерфейсу Dual-Stack осуществляется одним из двух выбранных вариантов:

1. Вариант подключения ОС к информационному ресурсу с использованием криптографического шлюза АПКШ «Континент»;

2. Вариант подключения ОС к информационному ресурсу с использованием абонентского пункта «Континент -АП».

Форма заявок в зависимости от выбранного варианта взаимодействия приведена
в приложении № 1 и № 2.

После осуществления подключения ОС по защищенному каналу к информационному ресурсу, ЦМУ ССОП ФГУП «ГРЧЦ» для подключения к API интерфейсу Dual-Stack передает ОС данные для настройки сервиса интеграции (см. раздел 4).

Контакты взаимодействия:

Почтовый адрес: ds\_info@noc.gov.ru

1. Регламент подключения
	1. **Вариант подключения ОС к информационному ресурсу с использованием криптографического шлюза АПКШ «Континент»**

Данный метод предполагает обмен сертификатами между ЦУС криптографической сети информационного ресурса и ЦУС внешней криптосети для построения ГОСТ VPN-туннеля.

Схема взаимодействия представлена на рисунке 1. 

Рисунок 1. Схема взаимодействия ОС с API Dual-Stack с использованием криптографического шлюза АПКШ «Континент»

ОС направляет заявку, по форме, указанной в Приложении №1 «Заявка на подключении к информационному ресурсу» на подключение к API Dual-Stack
в ЦМУ ССОП ФГУП «ГРЧЦ». В заявке должны быть отражены следующие данные:

* ФИО, должность Ответственного за защиту информации Оператора связи и его контактные данные;
* ФИО, должность Администратора СКЗИ Оператора связи и его контактные данные;
* Продукт для построения VPN, модель АПКШ «Континент» и версия установленного ПО;
* Внешний адрес VPN-туннеля (внешний адрес АПКШ «Континент»), сетевые объекты (защищаемые ресурсы), трансляция сети внутри VPN (виртуальные адрес) – необходимо согласовать с представителями технической поддержки;
* Матрицу доступа взаимодействия ОС с информационным ресурсом (IP-адресация сетей взаимодействия).

Сертификат ЦУС внешней криптографической сети оператора связи АПКШ «Континент», выпущенный по алгоритму «GOST34102012A» (формата X.509, кодировка base64).

ЦМУ ССОП ФГУП «ГРЧЦ» импортирует сертификат от ОС в ЦУС криптографической сети информационного ресурса, экспортирует и передает ответный сертификат ОС.

ОС в своем ЦУС импортирует присланный сертификат и формирует файл конфигурации разрешенных к доступу защищаемых сетей, ресурсов (расширение .nc). После чего направляет в ответном письме файл конфигурации в ЦМУ ССОП ФГУП «ГРЧЦ».

ЦМУ ССОП ФГУП «ГРЧЦ» импортирует файл конфигурации в ЦУС криптографической сети информационного ресурса, экспортирует файл конфигурации сети информационного ресурса (в нем указаны защищаемые сети, к которым будет осуществляться доступ из внешней криптографической сети ОС) и передает файл конфигурации ОС.

ОС импортирует присланный файл конфигурации в свой ЦУС после чего создается межсетевой ключ на основе публичных сертификатов криптографических сетей информационного ресурса и ОС, создает связь (туннель) со связанным АПКШ «Континент» информационного ресурса и проверяет канал связи средствами программы управления ЦУС или посредством запуска команды ping до сервера в защищаемой сети информационного ресурса.

После успешной проверки уведомляет ЦМУ ССОП ФГУП «ГРЧЦ» о том, что связь установлена.

* 1. **Вариант подключения ОС к информационному ресурсу с использованием абонентского пункта «Континент-АП»**

Вариант предполагает подключение ОС (внешнего участника взаимодействия) к API интерфейса Dual-Stack информационного ресурса с использованием технологии Remote-access VPN.

Со стороны ОС требуется установка программного обеспечения «Континент-АП» на сервер интеграции с необходимым набором средств защиты информации (далее – СрЗИ) - сертифицированные средства антивирусной защиты (далее – АВЗ), сертифицированная операционная система или наложенное средство защиты от несанкционированного доступа (далее – СрЗИ от НСД), средства доверенной загрузки (далее – АПМДЗ).

Со стороны организации, обслуживающей криптографическую сеть информационного ресурса, после получения и согласования заявки на подключение, требуется выпустить и переслать участнику внешнего взаимодействия конфигурационный файл для подключения «Континент-АП» к API интерфейсу Dual-Stack.

Ссылка для скачивания программного обеспечения «Континент-АП»:

<https://www.securitycode.ru/download_center/?section=downloads&product=Континент%20АП/ZTN&version=4>.

Схема взаимодействия приведена на рисунке 2.

 

Рисунок 2. Схема взаимодействия ОС с информационным ресурсом с использованием абонентского пункта «Континент-АП»

ОС отправляет запрос, по форме, указанной в Приложении №2 «Заявка на подключении к информационному ресурсу» в ЦМУ ССОП ФГУП «ГРЧЦ», на предоставление сертификата для «Континента-АП». ОС в своем запросе указывает:

* ФИО, должность Ответственного за защиту информации ОС и его контактные данные;
* Серийный номер АРМ;
* Наименование и версию используемого АВЗ;
* Наименование и версию СрЗИ от НСД;
* Серийный номер АПМДЗ;
* Внешний IP адрес VPN-туннеля.

ЦМУ ССОП ФГУП «ГРЧЦ» создает пользовательский сертификат «Континент-АП», экспортирует конфигурацию, включая ключевой контейнер, на неотчуждаемый носитель информации и направляет его ОС.

ОС подготавливает рабочее место, после чего устанавливает «Континент-АП» и загружает конфигурацию и ключевой контейнер с полученного носителя. Проверяет связь и уведомляет ЦМУ ССОП ФГУП «ГРЧЦ», о том, что связность установлена.

1. Данные для настройки сервиса интеграции с информационным ресурсом
2. Корневой сертификат (СА), с ограниченным сроком действия;
3. Файл конфигурации входа, который содержит конфигурацию для подключения с шифрованием и аутентификацией оператора по логину и паролю (SASL) к топику Kafka. Конфигурация приведена ниже:

sasl.jaas.config=org.apache.kafka.common.security.scram.ScramLoginModule required username="login" password="password";

security.protocol=SASL\_SSL

sasl.mechanism=SCRAM-SHA-512

1. IP-адрес и порт сервера брокера сообщений Kafka;
2. Наименование топика[[2]](#footnote-2), в который оператор будет отправлять справочники
Dual-Stack;
3. формат сообщений для отправки в топик в виде proto-файла:

message DualstackPair {

  enum operation\_code {

    ACQUIRE = 0;

    INTERIM = 1;

    RELEASE = 2;

  };

  // идентификатор пользовательского оборудования

  string abonent\_id = 1;

   // время жизни сведений по абоненту, в секундах

  uint32 ttl = 2;

   // IPv6 адрес

  string ip\_v6 = 3;

   // IPv4 адрес

  uint32 ip\_v4 = 5;

   // Код операции

  operation\_code operation = 6;

   // Unix time в миллисекундах

  uint64 timestamp = 7;

   // ID площадки

  uint32 site = 8;

}

Для проверки корректности работы интеграции с информационным ресурсом необходимо выполнить тестирование при помощи скрипта *kafka-console-producer.sh* из состава пакета программного обеспечения Kafka, который позволяет отправлять сообщения в топики Kafka из стандартного ввода консоли.

1. Заключительные положения
	1. **Изменения и пересмотр документа**

 Настоящие ТУ пересматриваются, изменяются и дополняются по мере необходимости, но не реже одного раза в три года.

 Проверка и пересмотр настоящих ТУ осуществляется в следующих случаях:

* при внедрении новых СрЗИ, существенно изменяющих порядок работы с ними;
* в случае изменения процессов обработки и защиты информации в ИС;
* при выявлении новых УБИ и определении необходимости реализации дополнительных защитных мер;
* по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности информации;
* при повышении класса (уровня) защищенности;
* по требованию представителей ФСБ России и ФСТЭК России.

ТУ подлежат обязательному пересмотру в случае изменения законодательства Российской Федерации в области ИБ.

ТУ подлежат полному пересмотру при изменении перечня решаемых задач, изменений конфигурации ИС, приводящих к существенным изменениям технологии обработки информации.

ТУ подлежат частичному пересмотру в остальных случаях.

 Вносимые изменения не должны противоречить другим разделам ТУ.

# Приложение № 1

к ТУ по подключению к защищенной сети информационного ресурса

посредством АПКШ «Континент»

**Заявка**

на подключении к информационному ресурсу.

Заявитель,

(полное наименование организации Заявителя)

в лице

(должность, фамилия, имя, отчество руководителя ОС)

просит Вас согласовать подключение нашей организации к информационному ресурсу (API Dual-Stack).

Исходная информация для организации подключения:

|  |  |  |
| --- | --- | --- |
| 1 | Наименование организации. |  |
| 2 | Ф.И.О. и должность Ответственного за защиту информации |  |
| 3 | Контактный телефон, E-mail Ответственного за защиту информации |  |
| 4 | Ф.И.О. и должность Администратора СКЗИ |  |
| 5 | Контактный телефон, E-mail Администратора СКЗИ |  |
| 6 | Модель АПКШ «Континент» |  |
| 7 | Внешний адрес VPN-туннеля (внешний адрес АПКШ «Континент») |  |
| 8 | Сетевые объекты (защищаемые ресурсы) |  |
| 9 | Сертификат межсетевого взаимодействия (приложить в виде файла .cer к заполненной анкете) |  |
| 10 | Трансляция сети внутри VPN (виртуальные адрес) |  |

 (должность) (подпись) (ФИО)

"\_\_\_" 20 г.

 М.П.

# Приложение № 2

к ТУ по подключению к защищенной сети информационного ресурса

с использованием абонентского пункта АПКШ «Континент -АП»

**Заявка**

на подключении к информационному ресурсу.

Заявитель,

(полное наименование организации Заявителя)

в лице

(должность, фамилия, имя, отчество руководителя ОС)

просит Вас согласовать подключение нашей организации на подключение к информационному ресурсу (API Dual-Stack).

Исходная информация для организации подключения:

|  |  |  |
| --- | --- | --- |
| 1 | Наименование организации: |  |
| 2 | Ф.И.О. Ответственного за защиту информации |  |
| 3 | Контактный телефон и E-mail Ответственного за защиту информации |  |
| 4 | Серийный номер АРМ: |  |
| 5 | Наименование и версию используемого АВЗ: |  |
| 6 | Наименование и версию СЗИ от НСД: |  |
| 7 | Серийный номер АПМДЗ ПАК «Соболь»: |  |
| 8 | Внешний адрес ГОСТ VPN-туннеля |  |

 (должность) (подпись) (ФИО)

"\_\_\_" 20 г.

 М.П.

1. Информационный ресурс в составе значимого объекта критической информационной инфраструктуры (ЗОКИИ) первой категории значимости. [↑](#footnote-ref-1)
2. ОС имеет доступ только к своему топику с правом на запись, без права на чтение. [↑](#footnote-ref-2)