**Требования к сети передачи данных участников информационного обмена**

Листов 27

**Москва 2024**

СОДЕРЖАНИЕ

[Обозначения и сокращения 3](#_Toc164188066)

[1 Общие положения 4](#_Toc164188067)

[2 Типизация схем подключения 5](#_Toc164188068)

[3 Рекомендуемые требования, обеспечиваемые при подключении Организаций к ЗСПД 7](#_Toc164188069)

[3.1 Рекомендации по номенклатуре используемых решений в Организации 7](#_Toc164188070)

[3.2 Рекомендации по номенклатуре решений, обеспечивающих необходимую пропускную способность каналов связи 8](#_Toc164188071)

[3.3 Рекомендации по обеспечению резервного электроснабжения 9](#_Toc164188072)

[3.4 Рекомендации по повышению надежности криптографической защиты каналов связи 9](#_Toc164188073)

[4 Обязательные требования, обеспечиваемые при подключении Организаций к ЗСПД 11](#_Toc164188074)

[4.1 Общие требования 11](#_Toc164188075)

[4.2 Требования к помещениям и организации защиты при размещении технических средств 12](#_Toc164188076)

[4.3 Требования к размещению ЦУС 13](#_Toc164188077)

[4.4 Требования к размещению сетевого оборудования и сетевой связности 14](#_Toc164188078)

[4.5 Требования по контролю конечных узлов Организации 16](#_Toc164188079)

[4.6 Организационные требования 17](#_Toc164188080)

[4.7 Требования при обнаружении аномальной активности на адресах Организации 18](#_Toc164188081)

[5 Формы технических сведений участников 20](#_Toc164188082)

Обозначения и сокращения

|  |  |
| --- | --- |
| **Аббревиатура** | **Наименование** |
| VPN | Виртуальная частная сеть (Virtual Private Network) |
| NAT | Преобразование сетевых адресов (Network Address Translation) |
| АС | Автоматизированная система |
| АПКШ | Аппаратно-программный комплекс шифрования |
| Государственная платформа | Единая цифровая платформа Российской Федерации «ГосТех» |
| ЗСПД | Защищенная сеть передачи данных |
| ИС | Информационная система |
| ИЭП | Инфраструктура электронного правительства |
| Оператор Государственной платформы | Федеральное казенное учреждение «Государственные технологии» |
| Оператор эксплуатации ИЭП | ПАО «Ростелеком», являющееся единственным исполнителем работ по эксплуатации инфраструктуры электронного правительства в соответствии с распоряжением Правительства Российской Федерации от 15.10.2009 № 1475-р |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| ПО | Программное обеспечение |
| СЗИ | Средства защиты информации |
| Ситуационный Центр | Федеральная государственная информационная система «Федеральный ситуационный центр электронного правительства» (сайт: <https://sc.digital.gov.ru>, почта: [sd@sc.digital.gov.ru](mailto:sd@sc.digital.gov.ru)) |
| ФСБ России | Федеральная служба безопасности Российской Федерации |
| ФСТЭК России | Федеральная служба по техническому и экспортному контролю Российской Федерации |
| ЦОД | Центр обработки данных |
| ЦУС | Центр управления сетью |
| ЭП | Электронная подпись |

# Общие положения

Защищенная сеть передачи данных СМЭВ предназначена для безопасного взаимодействия, управления и мониторинга распределенных информационных систем при использовании СМЭВ.

Данный документ определяет требования, соответствие которым необходимо обеспечить Организациям / ИС, подключаемым к ЗСПД СМЭВ.

# Типизация схем подключения

В рамках функционирования различных ИС, требующих в рамках ЗСПД обеспечения криптографической защиты данных при взаимодействии по открытым общедоступным сетям, необходимо организовывать подключение АС с различной архитектурой построения, расположения и назначения.

В части организации криптографической защиты передаваемых данных можно выделить ряд типовых схем подключения, применимых для существующих и перспективных информационных систем.

Большинство вариантов подключения к ЗСПД сводится к типовым и зависит от таких факторов, как количество подключаемых АРМ / серверов, необходимость резервирования, необходимость реализации на программно-аппаратных комплексах, уже имеющихся в наличии решений этого же вендора необходимой номенклатуры.

Типовые варианты подключения со стороны Организации / ИС в зависимости от вендора сводятся к следующим:

1. Использование продукции ViPNet Coordinator HW4 АО «ИнфоТеКС» в следующих модификациях и исполнениях:

* использование кластера ПАК ViPNet Coordinator HW5000\*;
* использование одиночного ПАК ViPNet Coordinator HW5000\*;
* использование кластера ПАК ViPNet Coordinator HW2000\*;
* использование одиночного ПАК ViPNet Coordinator HW2000\*;
* использование кластера ПАК ViPNet Coordinator HW100 C/ HW1000/ HW1000 С/ HW1000 D;
* использование одиночного ПАК ViPNet Coordinator HW50 A/ HW50 B/ HW100 C/ HW1000/ HW1000 С/ HW1000 D;

1. Использование продукции АПКШ «Континент» ООО «Код безопасности» в следующих модификациях и исполнениях:

* использование кластера Континент 3.9 IPC-3000F/ IPC-3000NF2/ IPC-R3000\*;
* использование одиночного Континент 3.9 IPC-3000F/ IPC-3000NF2/ IPC-R3000\*;
* использование кластера Континент 3.9 IPC-R50/ IPC-100/ IPC-R300/ IPC-R550/ IPC‑R800/ IPC-1000F/ IPC-1000NF2/ IPC-R1000;
* использование одиночного Континент 3.9 IPC-10/ IPC-R10/ IPC-R50/ IPC-100/ IPC‑R300/ IPC-R550/ IPC-R800/ IPC-1000F/ IPC-1000NF2/ IPC-R1000;

1. Использование продукции С-Терра Шлюз 4.3 ООО «С-Терра СиЭсПи» в следующих модификациях и исполнениях (не применяется для подключения субъектов Российской Федерации!):

* использование кластера С-Терра Шлюз 7000/ 8000\*;
* использование одиночного С-Терра Шлюз 7000/ 8000\*;
* использование кластера С-Терра Шлюз 100/ 1000/ 2000/ 3000;
* использование одиночного С-Терра Шлюз 100/ 1000/ 2000/ 3000;

1. Гибридная схема – симбиоз предыдущих вариантов.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\* - Использование Участником данных моделей ПАК (ViPNet Coordinator HW2000, ViPNet Coordinator HW5000, Континент 3.9 IPC-3000F, Континент 3.9 IPC-3000NF2, Континент 3.9 IPC-R3000, С-Терра Шлюз 7000 или С-Терра Шлюз 8000) для организации защищенного подключения к СМЭВ требует получения предварительного согласования со стороны Оператора СМЭВ и ОЭ ИЭП. Запрос на согласование должен содержать обоснование необходимости использования ПАК с повышенной производительностью, которая избыточна для подключения Участников к существующей защищенной сети СМЭВ.

# Рекомендуемые требования, обеспечиваемые при подключении Организаций к ЗСПД

На объектах информатизации (в Организациях), подключаемых к ЗСПД, должны быть реализованы требования по обеспечению информационной безопасности, регламентируемые текущим законодательством.

## Рекомендации по номенклатуре используемых решений в Организации

В таблице 1 представлены рекомендации по выбору типа ПАК ViPNet Coordinator HW4 в зависимости от количества используемых в подключаемой организации сетевых узлов (АРМ, серверов, терминалов), обрабатывающих подлежащую защите информацию.

Таблица 1 - Рекомендуемое оборудование в зависимости от количества АРМ

|  |  |  |
| --- | --- | --- |
| № п/п | Количество серверов, АРМ и терминалов в защищаемом сегменте | Рекомендуемая номенклатура решений АО «ИнфоТеКС» |
| 1 | до 6000 | ViPNet Coordinator HW5000 |
| 2 | до 5000 | ViPNet Coordinator HW2000 |
| 3 | до 1000 | ViPNet Coordinator HW1000 С/ HW1000 D |
| 4 | до 500 | ViPNet Coordinator HW1000 |
| 5 | до 10 | ViPNet Coordinator HW100 C |
| 6 | до 5 | ViPNet Coordinator HW50 A/ HW50 B |

В таблице 2 представлены рекомендации по выбору типа АПКШ «Континент» в зависимости от количества используемых в подключаемой организации сетевых узлов (АРМ, серверов, терминалов), обрабатывающих подлежащую защите информацию.

Таблица 2 - Рекомендуемое оборудование в зависимости от количества АРМ

|  |  |  |
| --- | --- | --- |
| № п/п | Количество серверов, АРМ и терминалов в защищаемом сегменте | Рекомендуемая номенклатура решений ООО «Код безопасности» |
| 1 | до 3000 | Континент 3.9 IPC-3000F/ IPC-3000NF2/ IPC-R3000 |
| 2 | до 1500 | Континент 3.9 IPC-R1000 |
| 3 | до 1000 | Континент 3.9 IPC-1000F/ IPC-1000NF2 |
| 4 | до 500 | Континент 3.9 IPC-R800 |
| 5 | до 150 | Континент 3.9 IPC-R550 |
| 6 | до 100 | Континент 3.9 IPC-100/ IPC-R300 |
| 7 | до 50 | Континент 3.9 IPC-R50 |
| 8 | до 5 | Континент 3.9 IPC-10/ IPC-R10 |

В таблице 3 представлены рекомендации по выбору типа С-Терра Шлюз 4.3 в зависимости от количества используемых в подключаемой организации сетевых узлов (АРМ, серверов, терминалов), обрабатывающих подлежащую защите информацию (не применяется для подключения субъектов Российской Федерации!).

Таблица 3 - Рекомендуемое оборудование в зависимости от количества АРМ

|  |  |  |
| --- | --- | --- |
| № п/п | Количество серверов, АРМ и терминалов в защищаемом сегменте | Рекомендуемая номенклатура решений ООО «С-Терра СиЭсПи» |
| 1 | более 1000 | С-Терра Шлюз 7000/ 8000 |
| 2 | до 1000 | С-Терра Шлюз 3000 |
| 3 | до 500 | С-Терра Шлюз 2000 |
| 4 | от 50 до 500 | С-Терра Шлюз 1000 |
| 5 | от 10 до 200 | С-Терра Шлюз 100 |

## Рекомендации по номенклатуре решений, обеспечивающих необходимую пропускную способность каналов связи

В таблице 4 представлены рекомендации по выбору типа ПАК ViPNet Coordinator HW4 в зависимости от необходимой пропускной способности при подключении Организации к ЗСПД.

Таблица 4 - Рекомендации по пропускной способности каналов связи

|  |  |  |
| --- | --- | --- |
| № п/п | Необходимая производительность шифрования | Рекомендуемая номенклатура решений АО «ИнфоТеКС» |
| 1 | до 10000 Мбит/с | ViPNet Coordinator HW5000 |
| 2 | до 6600 Мбит/с | ViPNet Coordinator HW2000 |
| 3 | до 2500 Мбит/с | ViPNet Coordinator HW1000 С/ HW1000 D |
| 4 | до 915 Мбит/с | ViPNet Coordinator HW1000 |
| 5 | до 175 Мбит/с | ViPNet Coordinator HW100 C |
| 6 | до 75 Мбит/с | ViPNet Coordinator HW50 A/ HW50 B |

В таблице 5 представлены рекомендации по выбору типа АПКШ «Континент» в зависимости от необходимой пропускной способности при подключении Организации к ЗСПД.

Таблица 5 - Рекомендации по пропускной способности каналов связи

|  |  |  |
| --- | --- | --- |
| № п/п | Необходимая производительность шифрования | Рекомендуемая номенклатура решений ООО «Код безопасности» |
| 1 | до 8000 Мбит/с | Континент 3.9 IPC-R3000 |
| 2 | до 6400 Мбит/с | Континент 3.9 IPC-3000F/ IPC-3000NF2 |
| 3 | до 5000 Мбит/с | Континент 3.9 IPC-R1000 |
| 4 | до 4400 Мбит/с | Континент 3.9 IPC-1000F/ IPC-1000NF2 |
| 5 | до 2500 Мбит/с | Континент 3.9 IPC-R800 |
| 6 | до 900 Мбит/с | Континент 3.9 IPC-R550 |
| 7 | до 500 Мбит/с | Континент 3.9 IPC-R300 |
| 8 | до 410 Мбит/с | Континент 3.9 IPC-100 |
| 9 | до 350 Мбит/с | Континент 3.9 IPC-R50 |
| 10 | до 200 Мбит/с | Континент 3.9 IPC-R10 |
| 11 | до 120 Мбит/с | Континент 3.9 IPC-10 |

В таблице 6 представлены рекомендации по выбору типа С-Терра Шлюз 4.3 в зависимости от необходимой пропускной способности при подключении Организации к ЗСПД (не применяется для подключения субъектов Российской Федерации!).

Таблица 6 - Рекомендации по пропускной способности каналов связи

|  |  |  |
| --- | --- | --- |
| № п/п | Необходимая производительность шифрования | Рекомендуемая номенклатура решений ООО «С-Терра СиЭсПи» |
| 1 | до 9290 Мбит/с | С-Терра Шлюз 8000 |
| 2 | до 5710 Мбит/с | С-Терра Шлюз 7000 |
| 3 | до 1510 Мбит/с | С-Терра Шлюз 3000 |
| 4 | до 1060 Мбит/с | С-Терра Шлюз 2000 |
| 5 | до 405 Мбит/с | С-Терра Шлюз 1000 |
| 6 | до 150 Мбит/с | С-Терра Шлюз 100 |

## Рекомендации по обеспечению резервного электроснабжения

При подключении ПАК к UPS последний обеспечивает работу ПАК только до тех пор, пока не разрядится батарея. После разряда батареи ПАК будет некорректно выключен, что может привести к потере данных. В то же время большинство современных UPS могут подключаться к ПАК с помощью интерфейсного кабеля и посылать сигнал об истощении батареи. Полученный сигнал ПАК может использовать для корректного выключения.

## Рекомендации по повышению надежности криптографической защиты каналов связи

Повышение надежности криптографической защиты каналов связи может быть обеспечено путем установки холодного резерва в дополнительном ЦОД. Для этого в первом ЦОД должен быть настроен ПАК1 (одиночный/кластер), во втором ЦОД - ПАК2 того же производителя. ПАК2 должен быть отключен (либо включен, но для него отключен канал на стороне Организации).

В случае возникновения нештатной ситуации с ПАК1 осуществляется ручное включение ПАК2 сотрудниками Организации. ПАК1 при этом необходимо отключить.

Одновременно ПАК1 и ПАК2 включать запрещено, т.к. это приведет к возникновению взаимного аффекта.

При использовании данной схемы с оборудованием ViPNet Coordinator HW4 должна совпадать модель оборудования, а также туннелируемые ip-адреса (пункт 6 в таблице 11).

Для оборудования С-Терра Шлюз 4.3 на внешних интерфейсах должны быть назначены серые ip-адреса (пункт 1 таблицы 11), и они должны транслироваться в один и тот же публичный адрес (пункт 3 таблицы 11). Модель оборудования для холодного резерва может отличаться от основной.

Для оборудования АПКШ «Континент» модель оборудования и вся адресация должны полностью совпадать. Отличаться может только публичный адрес трансляции (пункт 3 таблицы 11).

# Обязательные требования, обеспечиваемые при подключении Организаций к ЗСПД

## Общие требования

Во исполнение требований законодательства РФ и других нормативных документов в области обеспечения ИБ для организации защищённого информационного обмена следует обеспечивать криптографическую защиту каналов связи, проходящих через неконтролируемую зону, в том числе по открытым общедоступным сетям.

В СМЭВ для организации криптографической защиты каналов связи при взаимодействии информационных систем используются продуктовые линейки производства компаний «Инфотекс», «Код безопасности» и «С-Терра СиЭсПи» (возможность использования продукции компании «С-Терра СиЭсПи» для подключения субъектов Российской Федерации не предусмотрена!). Все Организации, подключаемые к ЗСПД СМЭВ, для обеспечения совместимости СКЗИ обязаны использовать СКЗИ данного типа.

Централизованное управление и мониторинг СКЗИ осуществляются силами ПАО «Ростелеком», являющегося единственным исполнителем работ по эксплуатации инфраструктуры электронного правительства. Подключаемая организация на период действия Договора по техническому обслуживанию защищенного соединения передает полное управление СКЗИ специалистам ПАО «Ростелеком».

Данные СКЗИ имеют сертификат соответствия ФСБ России до уровня КС3 включительно. При подключении к СМЭВ комплектация оборудования должна соответствовать уровня КС3.

В случае если в подключаемой Организации используются СКЗИ другого производителя, следует обеспечивать перешифрование трафика из СКЗИ другого производителя на СКЗИ представленных выше производителей.

Оборудование Организаций настраивается и подключается к уже развернутой защищенной сети ИЭП.

Для поставщиков сведений действует дополнительное обязательное требование к оборудованию – наличие горячего резервирования.

Оператор эксплуатации ИЭП обеспечивает отдельный выделенный защищенный канал связи до экземпляра Государственной платформы (отдельный кластер оборудований, СКЗИ, защищенные сети с ЦУС). Использование данного защищенного канала в иных целях запрещено.

Оператор Государственной платформы подключается к СМЭВ, соблюдая все требования, предусмотренные настоящим документом, и имеет возможность предоставления доступа к ЗСПД СМЭВ другим Организациям, которые размещены на экземпляре Государственной платформы, по отдельной адресации доступа.

## Требования к помещениям и организации защиты при размещении технических средств

При размещении технических средств (ТС) на объектах информатизации Организаций следует руководствоваться Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66, Инструкцией 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, утвержденной приказом ФАПСИ от 13 июля 2001 г. № 152, эксплуатационной и технической документацией на используемые средства криптографической защиты информации, а также следующими требованиями:

1. Размещение, охрана и специальное оборудование помещений, в которых установлены ТС и ведется работа с носителями персональной ключевой информации, должны исключать возможность бесконтрольного проникновения в них посторонних лиц, прослушивания ведущихся там переговоров и просмотра помещений посторонними лицами, а также гарантировать сохранность находящихся в этих помещениях конфиденциальных документов.
2. На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством учреждения, в которых предусматривается порядок вызова администрации, должностных лиц, вскрытие помещений, очередность и порядок эвакуации конфиденциальных документов и дальнейшего их хранения.
3. Технические средства могут подключаться к общегородской сети электроснабжения с учетом требований инструкций по эксплуатации вычислительных средств и правил техники безопасности.
4. Оборудование помещений средствами вентиляции и кондиционирования воздуха должно соответствовать санитарно-гигиеническими нормам СНиП, устанавливаемым законодательством Российской Федерации.
5. При подключении СКЗИ к каналам передачи данных, выходящим за пределы контролируемой зоны, необходимо выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К). При монтаже каналов связи, гальванические цепи которых непосредственно от ПЭВМ (с установленным на нем СКЗИ) выходят за пределы контролируемой территории, должны использоваться оптоволоконные развязки.
6. При использовании СКЗИ только для выполнения функций генерации/проверки ЭП, а также если подключение к каналам передачи данных, выходящих за пределы контролируемой зоны, осуществляется через активное канальное оборудование (находящееся в пределах контролируемой зоны), использование оптоволоконной развязки не требуется.

## Требования к размещению ЦУС

Текущие типовые схемы подключения к ЗСПД не предусматривают размещения Центра управления сетью на объектах информатизации Организаций. Под ЦУС подразумеваются решения разных производителей, имеющих разные названия: ViPNet Администратор, ПУ ЦУС, С‑Терра КП. Однако в случае принятия данного решения (изменение требований законодательства, специфичная архитектура ИС, иные мотиваторы) необходимо обеспечивать выполнение следующих требований:

1. Помещения, в которых устанавливаются компоненты ЦУС, относятся к защищаемым помещениям, обеспечивающим конфиденциальность проводимых работ и исключающим возможность бесконтрольного нахождения в нем посторонних лиц.
2. Входные двери помещений должны быть оборудованы внутренними замками, гарантирующими надежное закрытие дверей при выходе из помещения и в нерабочее время. Окна (при необходимости) и двери должны быть оборудованы охранной сигнализацией, связанной с центральным пультом наблюдения за сигнализацией поста охраны.
3. Служебные помещения Удостоверяющего центра, используемые для архивного хранения документов на бумажных, магнитных и оптических носителях, оборудуются средствами вентиляции и кондиционирования воздуха, обеспечивающими соблюдение установленных параметров температурно-влажностного режима, вентиляции и очистки воздуха.
4. В помещение допускаются только сотрудники, имеющие непосредственное отношение к организации эксплуатации ЦУС.
5. Уборка помещения, обслуживание оборудования систем жизнеобеспечения осуществляется назначенным персоналом при выключенных мониторах в присутствии администратора.
6. Должны быть приняты меры по надежному сохранению в тайне паролей доступа, ключевых дистрибутивов и другой ключевой информации, размещенной на съемных носителях. Для хранения съемных носителей помещение должно быть оборудовано сейфом.
7. По окончании рабочего дня помещения закрываются, опечатываются и сдаются под охрану. Порядок сдачи помещений определяется эксплуатирующей организацией.

## Требования к размещению сетевого оборудования и сетевой связности

При размещении сетевого оборудования, размещаемого на объектах информатизации, подключаемых к ЗСПД, Организации необходимо выполнить следующее:

1. Обеспечить физическое размещение оборудования, в зависимости от марки и модели оборудования:

* для ViPNet Coordinator HW2000/ HW5000 одно место размером 19 дюймов Rack 1U (для установки в стойку) 430 x 44 x 476 мм (ШхВхГ);
* для ViPNet Coordinator HW1000/ HW1000 C/ HW1000 D одно место размером 19 дюймов Rack 1U (для установки в стойку) 430 x 44 x 453 мм (ШхВхГ);
* для ViPNet Coordinator HW100 C место размером 174 x 44 x 138 мм (ШхВхГ);
* для ViPNet Coordinator HW50 A/ HW50 B место размером 125 x 20 x 120 мм (ШхВхГ);
* для Континент 3.9 IPC-3000F/ IPC-3000NF2 одно место размером 19 дюймов Rack 1U (для установки в стойку) 438 x 45 x 583 мм (ШхВхГ);
* для Континент 3.9 R3000/ IPC-1000F/ IPC-1000NF2/ R1000/ R800 одно место размером 19 дюймов Rack 1U (для установки в стойку) 430 x 45 x 500 мм (ШхВхГ);
* для Континент 3.9 R300/ R550 место размером 180 x 45 x 175 мм (ШхВхГ);
* для Континент 3.9 IPC-100 место размером 437 x 45 x 417 мм (ШхВхГ);
* для Континент 3.9 R10/ R50 место размером 180 x 45 x 140 мм (ШхВхГ);
* для Континент 3.9 IPC-10 место размером 220 x 30 x 143 мм (ШхВхГ);
* для С-Терра Шлюз 7000/ 8000 одно место размером 19 дюймов Rack 1U (для установки в стойку) 438 х 44 x 630 мм (ШхВxГ);
* для С-Терра Шлюз 3000 одно место размером 19 дюймов Rack 1U (для установки в стойку) 438 х 44 x 525 мм (ШхВxГ);
* для С-Терра Шлюз 1000/ 2000 одно место размером 19 дюймов Rack 1U (для установки в стойку) 431 х 44 x 305 мм (ШхВxГ);
* для С-Терра Шлюз 100 одно место размером 125 х 20 x 120 мм (ШхВxГ).

1. Обеспечить подключение оборудования максимальной потребляемой мощностью 270 Вт к сети гарантированного электропитания питания 220 В с помощью кабеля типа С13 – СЕЕ7/7 (евровилка).
2. Обеспечить возможность подключения к сетевому оборудованию интерфейсов криптомаршрутизатора с использованием интерфейсов Ethernet Base T 100/1000.
3. Обеспечить связность на втором уровне модели OSI/ISO внутренних интерфейсов криптошлюзов при кластерном подключении, т. е. разместить два физических интерфейса в одном широковещательном сегменте.
4. При подключении через сеть Интернет обеспечить доступность внешнего интерфейса криптошлюза (внешний «белый» IP адрес) из сети Интернет одним из следующих способов:

* обеспечение NAT-трансляции частного IP-адреса в публичный IP-адрес и публичного IP-адреса в частный по протоколам TCP, UDP и портам в соответствии с таблицей 7.

Таблица 7 –Таблица необходимых портов и протоколов для функционирования криптообрудования

|  |  |  |  |
| --- | --- | --- | --- |
| Оборудование | Протокол | Порт | Примечание |
| ViPNet | UDP | 55777 | Разрешить прохождение в обе стороны |
| С-Терра | UDP | 500, 4500 | Разрешить прохождение в обе стороны |
| АПКШ Континент | UDP | 123, 161, 4433, 5100-5101, 5106-5107, 5109, 5557, 7500, 10000-10031 | Разрешить прохождение в обе стороны |
| АПКШ Континент | TCP | 22, 4431, 4444-4446, 5100-5101, 5103, 5109, 7500 | Разрешить прохождение в обе стороны |

* выделение для интерфейса публичного IP-адреса.

1. Обеспечить отсутствие логических препятствий для прохождения трафика по протоколу UDP, TCP и портам между внешним интерфейсом криптошлюза (ip внеш.) и адресами криптошлюзов ИС. Список портов указан в таблице 7.
2. Обеспечить маршрутизацию в локальной сети Организации таким образом, чтобы трафик с адресов серверов Организации, отправляемый через ЗСПД, направлялся на внутренний интерфейс криптомаршрутизатора;
3. При подключении АРМ для каждой Организации, которые виртуализируются средствами СКЗИ, предусматривается выделение до 8[[1]](#footnote-2) IPv4-адресов (1 адрес на 1 АРМ, сервер и прочие вычислительные узлы, входящие в ЗСПД СМЭВ на стороне Организации);
4. Проксирование/маскирование/трансляция сетевых адресов/портов, выделенных для Организации, разрешается только внутри Организации (одного юридического лица).

## Требования по контролю конечных узлов Организации

Доступ к СМЭВ предоставляется участникам межведомственного взаимодействия при наличии подтверждения выполнения в информационной системе участника межведомственного взаимодействия предъявленных к ней требований по защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

С целью информирования о защите конечных узлов Организация предоставляет[[2]](#footnote-3) Оператору эксплуатации ИЭП сведения по форме[[3]](#footnote-4), приведённой в таблице 8.

Таблица 8 - Форма сведений о защите конечных узлов Участника

|  |  |
| --- | --- |
| **Форма сведений о защите конечных узлов Участника** | |
| **Полное и сокращенное наименование Организации** |  |
| Перечень установленного ПО (версия, сборка, релиз и пр.) |  |
| Подтверждение отсутствия использования нелицензионного ПО |  |
| Подтверждение наличия сертифицированной регуляторами Российской Федерации ОС (наименование, версия, сборка) |  |
| Подтверждение установки актуальных обновлений ОС, в т.ч. обновлений безопасности |  |
| Подтверждение реализации периодической установки обновлений ОС, в т.ч. обновлений безопасности |  |
| Подтверждение реализации поддержки антивирусных баз данных в актуальном состоянии |  |
| Подтверждение реализации мер по изоляции программной среды |  |
| Подтверждение реализации мер по защите от несанкционированного доступа к конечному узлу |  |
| Файлы отчетов проведения инструментального контроля подключаемого конечного узла (первичный и после устранения критических недостатков/уязвимостей). |  |

## Организационные требования

Подключенная к СМЭВ Организация обязуется:

1. В случае проведения работ на стороне Организации, которые могут привести к недоступности криптооборудования, используемого для подключения к СМЭВ, оповестить Службу технической поддержки СМЭВ посредством направления запроса в Ситуационный центр (<https://sc.digital.gov.ru> или [sd@sc.digital.gov.ru](mailto:sd@sc.digital.gov.ru)) о сроках проведения данных работ. Оповещение в Службу технической поддержки СМЭВ должно быть направлено не менее чем за 2 рабочих дня до начала работ на стороне Организации.
2. В случае изменения контактной информации сотрудников Организации, ответственных за криптооборудование, направить актуальные сведения в Службу технической поддержки СМЭВ через запрос в Ситуационный центр (<https://sc.digital.gov.ru> или [sd@sc.digital.gov.ru](mailto:sd@sc.digital.gov.ru)). Актуальные сведения в Службу технической поддержки СМЭВ должны быть направлены не позднее 2 рабочих дней с момента изменения контактной информации сотрудников Организации, ответственных за криптооборудование.
3. Выполнять требования Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденного приказом ФСБ России от 9 февраля 2005 г. № 66, 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, утвержденной приказом ФАПСИ от 13 июля 2001 г. №152, эксплуатационной и технической документации на используемые средства криптографической защиты информации.

## Требования при обнаружении аномальной активности на адресах Организации

При обнаружении инцидентов ИБ на адресах, используемых Организацией для подключения к СМЭВ, Оператор эксплуатации ИЭП блокирует подключение Организации и направляет уведомление в Ситуационный Центр, а также в Организацию. Уведомление в Ситуационный Центр содержит сведения о блокировке доступа к СМЭВ для Организации (с указанием адресов подключения). Уведомление в сторону Организации содержит требование о предоставлении причин возникновения инцидента ИБ и указания мероприятий для устранения инцидента ИБ. После получения ответов от Организации Оператор эксплуатации ИЭП принимает решение (на основании достаточности и корректности ответов) о разблокировке подключения Организации.

Сроки разблокировки подключения Организации зависят от количества блокировок, фиксируемых в течение одного календарного месяца, и представлены в таблице 9.

Таблица 9 – Сроки разблокировки подключения Организации

|  |  |  |
| --- | --- | --- |
| № п/п | Количество блокировок в одном календарном месяце | Срок разблокировки |
|  | 1 | По запросу от Организации, после предоставления ответа согласно пункту 4.6 |
|  | 2 | Через 1 календарный день, после предоставления ответа согласно пункту 4.6 |
|  | 3 | Через 7 календарный дней, после предоставления ответа согласно пункту 4.6 |
|  | 4 и более | Только после письменного согласования со стороны Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации на основании официального обращения Организации |

# Формы технических сведений участников

При подключении Организации к ЗСПД необходимо предоставить сведения по формам, приведённым в таблицах 8, 10, 11 и 12.

При необходимости внесения изменений в уже настроенное подключение к ЗСПД необходимо предоставить сведения по форме, приведённой в таблице 13.

Таблица 10 - Форма технических сведений Участника

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование** | |  | | | | | | | | | | |
| **Статус** | | **Федеральный** | | | | | **Региональный** | | | | | |
|  | | | | |  | | | | | |
| **Почтовый адрес** | |  | | | | | | | | | | |
| **Юр. Адрес** | |  | | | | | | | | | | |
| **Потребность в услугах ЭП** | | *Перечислить цели подключения к ЦОД* | | | | | | | | | | |
| **Контактные данные** | | **Рабочий телефон** | | | **Мобильный телефон** | | | | **Е-mail** | | | |
| **Адм. лицо, ответственное за подключение** | |  | | |  | | | |  | | | |
| **ФИО** |  |
| **Сетевой инженер** | |  | | |  | | | |  | | | |
| **ФИО** |  |
| **Лицо, ответственное за ИБ** | |  | | |  | | | |  | | | |
| **ФИО** |  |
| **Объект подключения** | | **Адрес** | | | **Этаж** | | | | **Помещение** | | | |
|  | | |  | | | |  | | | |
| **Наличие подключения** | | **Интернет** | | | **IP/MPLS сеть**  **ПАО «Ростелеком»** | | | | **Отсутствует** | | | |
|  | | |  | | | |  | | | |
| **Предпочтительный вариант подключения** | |  | | |  | | | |  | | | |
| **Предпочтительная типовая схема подключения согласно рисунку 1 или 2** | | **1** | | | | | **2** | | | | | |
|  | | | | |  | | | | | |
| **Параметры имеющегося оборудования** | | **Тип** | | | **Интерфейс** | | | | **Параметры** | | | |
| Коммутатор Ethernet | |  | | |  | | | |  | | | |
| Граничный маршрутизатор ЛВС | |  | | |  | | | |  | | | |
| **Наличие и тип имеющегося для подключения оборудования ViPNet** | | HW1000 | | HW100A | | | HW100B | | | HW100C | | |
|  | |  | | |  | | |  | | |
| **Кол-во оборудования ViPNet используемого конкретно для подключения к ИЭП ПАО «Ростелеком»** | |  | |  | | |  | | |  | | |
| **Потребность в закупке оборудования ViPNet через ПАО «Ростелеком»** | |  | |  | | |  | | |  | | |
| **Наличие и тип имеющегося для подключения оборудования АПКШ Континент** | | IPS 3000 | IPS 1000 | | | IPS 100 | | IPS 25 | | | | IPS 10 |
|  |  | | |  | |  | | | |  |
| **Кол-во оборудования АПКШ Континент используемого конкретно для подключения к ИЭП ПАО «Ростелеком»** | |  |  | | |  | |  | | |  | |
| **Потребность в закупке оборудования АПКШ Континент через ПАО «Ростелеком»** | |  |  | | |  | |  | | |  | |
| **Наличие и тип имеющегося для подключения оборудования С-Терра** | | GATE  7000\GATE 3000 | GATE 1000V | | | GATE 100V | | GATE 100 | | | GATE 100B | |
|  |  | | |  | |  | | |  | |
| **Кол-во оборудования С-Терра используемого конкретно для подключения к ИЭП ПАО «Ростелеком»** | |  |  | | |  | |  | | |  | |
| **Потребность в закупке оборудования С-Терра через ПАО «Ростелеком»** | |  |  | | |  | |  | | |  | |
| **Лицензионные номера** | |  | | | | | | | | | | |
| **Заводской номер** | |  | | | | | | | | | | |

Таблица 11 - Форма технических сведений участника (оборотная сторона)

|  |  |  |
| --- | --- | --- |
| № | IP адрес/маска | Назначение |
| 1  1.1  1.2  1.3 | IP внеш./маска | IP-адрес и маска сети внешнего интерфейса криптошлюза. Может быть как из частного, так и из публичного адресного пространства.  В случае отказоустойчивого кластера должны быть выделены 3 адреса одной подсети.  В случае подключения через IP/MPLS-сеть ПАО «Ростелеком» данные адреса не указываются. |
| 2 | IP gw внеш. | Адрес шлюза по умолчанию в сети, в которую включается внешний интерфейс криптошлюза.  В случае подключения через IP/MPLS-сеть ПАО «Ростелеком» данные адреса не указываются. |
| 3 | IP fw (NAT) | Публичный Интернет адрес NAT-трансляции, через который осуществляется доступ к внешнему интерфейсу криптошлюза.  Указывается в случае использования частного адреса на внешнем интерфейсе криптошлюза при подключении через сеть Интернет. |
| 4  4.1  4.2  4.3 | IP внут./маска | Адрес и маска сети внутреннего интерфейса криптошлюза.  В случае отказоустойчивого кластера должны быть выделены 3 адреса одной подсети.  IP внеш. и IP внут. обязательно должны принадлежать разным подсетям. |
| 5 | IP gw внут. | Адрес шлюза для доступа к внутренним ресурсам ведомства.  Указывается в случае нахождения ресурсов ведомства и внутреннего интерфейса криптошлюза в разных сетях. |
| 6 | IP сер. | Адрес(а) сервера(ов) Организации, которые будут взаимодействовать через ЗСПД. |

Параметры адресации, указанные на оборотной стороне Формы технических сведений Участника, зависят от выбранной схемы подключения и должны соответствовать приведённым на рисунке 1 и рисунке 2.

Параметры адресации при использовании кластерного или одиночного решения различаются между собой, что отражено на соответствующих схемах:

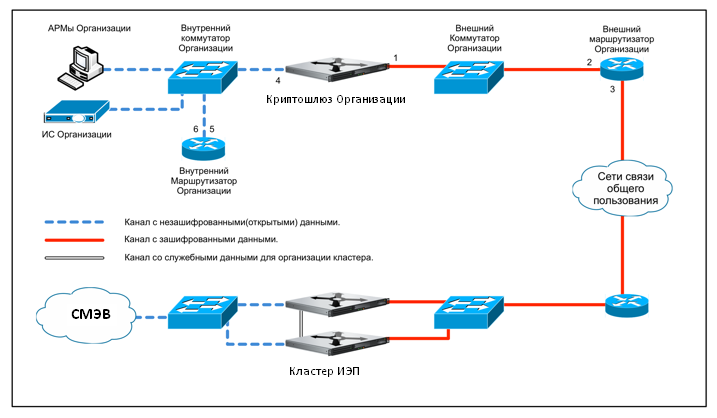


Рисунок 1 - Адресация при использовании одиночного решения

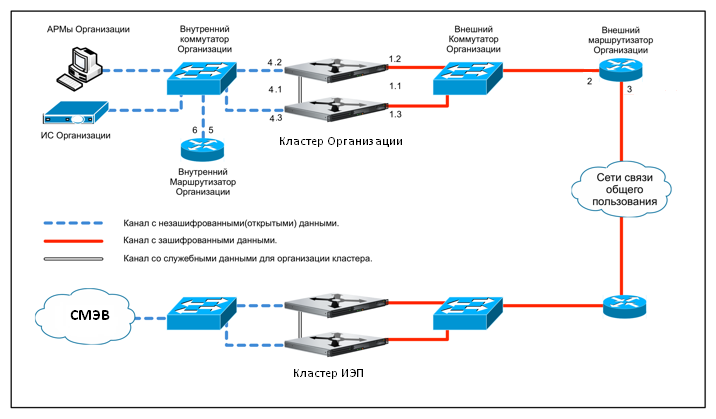


Рисунок 2 - Адресация при использовании кластерного решения

Таблица 12 - Форма сведений об IP-адресах, наименовании и мнемонике ИС Участника

|  |  |  |  |
| --- | --- | --- | --- |
| **Форма для нового Участника** | | | |
| **Полное и сокращенное наименование Организации** | |  | |
|  | **IP конечных узлов** | **Наименование ИС** | **Мнемоника ИС** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Таблица 13- Форма для корректировки сведений Участника

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Форма для корректировки сведений Участника** | | | | | | | | | | | | | |
| **Полное и сокращенное наименование Организации** | | |  | | | | | | | | | | |
| **Серийные и лицензионные номера каналообразующего криптооборудования СМЭВ[[4]](#footnote-5)** | | |  | | | | | | | | | | |
| **Выбрать тип запроса:** | **IP конечных узлов** | | | **Наименование ИС** | | **Мнемоника ИС** | | **Новая запись[[5]](#footnote-6)** | | | | | |
| **IP** | | **Наименование ИС** | | **Мнемоника ИС** | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |
| Выберите элемент. |  |  | | |  | |  | |  | |  | |  | |

Лист регистрации изменений

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Изм. | Номера листов (страниц) | | | | Всего  листов  (страниц)  в докум. | №  докум. | Входящий  № сопрово-  дительного  документа  и дата | Подпись | Дата |
| изменён-ных | заменен-ных | новых | изъятых |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

1. Для Государственной платформы предусматривается выделение до 8 IPv4-адресов на одну Организацию [↑](#footnote-ref-2)
2. Оператор государственной платформы транслирует Оператору эксплуатации ИЭП сведения, получаемые от Участников по **форме сведений о защите конечных узлов Участника**. [↑](#footnote-ref-3)
3. При изменении любых сведений из ранее указанных в **форме сведений о защите конечных узлов Участника,** на стороне Организации Участник обязан направить обновленные сведения. [↑](#footnote-ref-4)
4. Заполняется для идентификации каналообразующего криптооборудования Участника [↑](#footnote-ref-5)
5. Заполняется только при выборе типа запроса **- Внесение изменений** [↑](#footnote-ref-6)