Регламент подключения к защищенной виртуальной сети Муниципального автономного учреждения «Центр муниципальных информационных ресурсов и технологий»

1. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

Администратор СКЗИ – работник органа криптографической защиты назначенный ответственным за обеспечение функционирования и безопасности СКЗИ в информационной инфраструктуре МАУ «ЦМИРиТ».

Дистрибутив ключей – файл с расширением. DST, в этом файле помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив справочно-ключевой информации необходимо установить на сетевой узел.

Доверенный способ передачи информации — способ передачи информации, принятый двумя или несколькими юридическими лицами на основе взаимной договоренности и обеспечивающий требуемую степень её защищенности.

Защищенная виртуальная сеть – технология, позволяющая создать логическую сеть, чтобы обеспечить множественные сетевые соединения между компьютерами или локальными сетями через существующую физическую сеть. Уровень доверия к такой виртуальной сети не зависит от уровня доверия к физическим сетям благодаря использованию средств криптографии (шифрования, аутентификации и средств персонального и межсетевого экранирования).

Информационная система (ИС) – это взаимосвязанная совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации для достижения цели управления.

Ключевой документ - физический носитель определённой структуры, содержащий ключевую информацию (исходную ключевую информацию), а при необходимости - контрольную, служебную и технологическую информацию.

Ключевая информация - совокупность данных, предназначенных для выработки по определённым правилам криптоключей; Ключевая информация - специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определённого срока;

Ключевой носитель - физический носитель определённой структуры, предназначенный для размещения на нем ключевой информации (исходной ключевой информации).

Компрометация – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, связанные с криптоключами и ключевыми носителями, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Межсетевое взаимодействие – информационное взаимодействие, организованное между сетями ViPNet. Позволяет узлам различных сетей ViPNet обмениваться информацией по защищенным каналам. Для организации взаимодействия между узлами различных сетей ViPNet администраторы этих сетей обмениваются межсетевой информацией.

Межсетевая информация - Информация о доверенной сети или своей сети, предназначенная для организации или изменения межсетевого взаимодействия. В состав межсетевой информации входят связи между сетевыми объектами, параметры сетевых узлов ViPNet и служебная информация (сертификаты издателей, списки аннулированных сертификатов).

Межсетевой мастер-ключ -- ключ, служащий для формирования ключей обмена между сетевыми узлами разных криптосетей.

Орган криптографической защиты (ОКЗ) –функциональный орган Учреждения, работник Учреждения или стороннее юридическое лицо, на которое возложены обязанности по разработке и осуществлении мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации ограниченного доступа.

Ответственный за организацию работ по криптографической защите информации (Ответственный пользователь СКЗИ) – сотрудник Учреждения, отвечающий за реализацию мероприятий, связанных с обеспечением в Учреждении безопасности хранения, учета, обработки и передачи по каналам связи с использованием СКЗИ информации ограниченного доступа. В МАУ «ЦМИРиТ» Ответственным пользователем СКЗИ является ведущий инженер сектора по безопасности и защите информации.

Пользователь Vipnet – это лицо, зарегистрированное на сетевом узле Vipnet.

Пользователь СКЗИ – работник Учреждения, непосредственно допущенный к работе с СКЗИ.

Претендент – организация, имеющая намерения подключиться к Защищенной сети.

Программное обеспечение (ПО) – программа или набор программ для ЭВМ (компьютера, автоматизированного рабочего места).

Средства защиты информации (СЗИ) – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

Средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

Средство криптографической защиты информации (СКЗИ) - совокупность аппаратных и(или) программных компонентов, предназначенных для подписания электронных документов и сообщений электронной подписью, шифрования этих документов при передаче по открытым каналам, защиты информации при передаче по каналам связи, защиты информации от несанкционированного доступа при её обработке и хранении.

Узел ViPNet - рабочее место, на котором будет установлено ПО ViPNet Client для работы в Защищенной сети, с помощью которого защищают информацию приложений ViPNet, хранимую локально на компьютере, и (или) трафик, посредством шифрования, имитозащиты и ЭП.

Участник – организация, подключенная к Защищенной сети в установленном в настоящем регламенте порядке.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

IP-адрес – Адрес узла в сети, построенной на основе протокола IP.

ITSM (IT Service Management, управление ИТ-услугами) – система управления ИТ службой МАУ ЦМИРиТ, осуществляющая прием, регистрацию и выполнение заявок участников, реагирование на инциденты, а также ведение учета IT- активов.

URL – это уникальный адрес, который ведет на ресурс в защищенной виртуальной сети.

2. ВВЕДЕНИЕ

2.1. Обзорная информация

Настоящий Регламент подключения к защищенной виртуальной сети муниципального автономного учреждения «Центр муниципальных информационных ресурсов у технологий» (далее - Регламент) определяет механизмы, условия подключения к защищенной сети, включая обязанности участников защищенной сети, основные организационно-технические мероприятия, необходимые для безопасной работы защищенной сети.

2.2. Идентификация Регламента

Наименование документа: «Регламент подключения к защищенной виртуальной сети муниципального автономного учреждения «Центр муниципальных информационных ресурсов у технологий».

Версия: 1.0.

Дата: 19.02.2022 г.

2.3. Публикация Регламента

Настоящий Регламент распространяется в электронной форме на сайте по адресу https://cmirit.ru/documents

2.4. Срок действия Регламента

Настоящий Регламент вступает в силу со дня его утверждения руководителем муниципального автономного учреждения «Центр муниципальных информационных ресурсов у технологий» (далее - МАУ «ЦМИРиТ»).

Срок действия Регламента - 5 лет.

Если Орган криптографической защиты (далее - ОКЗ) официально не уведомит пользователей о прекращении действия Регламента, то Регламент автоматически пролонгируется на следующие 5 лет.

Официальное уведомление о прекращении действия Регламента осуществляется способами, определенными в разделе публикация Регламента:

Копии уведомления, предназначенные для распространения в электронной форме на сайте МАУ «ЦМИРиТ» https://cmirit.ru/documents

2.5. Контактная информация

Муниципальное автономное учреждение «Центр муниципальных информационных ресурсов у технологий»: Вологодская обл. г. Череповец, ул. Набережная, 29 «Д».

Контактный телефон Администратора СКЗИ: 8(8202)55-15-25 доб. 1046.

Контактный телефон Руководителя ОКЗ: 8(8202)55-15-25 доб. 1050.

E-mail Администратора СКЗИ: bizi@cherepovetscity.ru

2.6. Изменение Регламента

2.6.1. Извещение о вносимых изменениях

Проект регламента подключения к Защищенной виртуальной сети МАУ «ЦМИРиТ» с изменениями и дополнениями за 30 дней до его утверждения размещается на сайте https://cmirit.ru/documents

2.6.2. Процедуры утверждения Регламента

Регламент подключения к Защищенной виртуальной сети МАУ «ЦМИРиТ» утверждается руководителем учреждения.

2.6.3. Процедура опубликования

ОКЗ в течение 5 рабочих дней с момента утверждения Регламента размещает Регламент на сайте https://cmirit.ru/documents

ОКЗ обеспечивает доступность действующего Регламента для своих пользователей на сайте https://cmirit.ru/documents

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Регламент подключения к защищенной виртуальной сети ViPNet №2317 МАУ «ЦМИРиТ» разработан в соответствии с:

- Федеральным законом от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- приказом ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

- приказом 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»;

- иными нормативными актами, регулирующими отношения в области защиты информации.

3.2. Назначение Защищенной сети

Защищенная сеть предназначена для обеспечения информационной безопасности при работе в защищенных сегментах государственных информационных систем, в региональной системе межведомственного электронного взаимодействия, в единой централизованной информационной системы бюджетного (бухгалтерского) учета и отчетности, а также в системе 1С-Зарплата и кадры.

3.3. Регламент определяет и устанавливает:

- порядок организации подключения Участников Защищенной сети (далее - Участники) к защищенной виртуальной сети ViPNet 2317 МАУ «ЦМИРиТ» (далее - Защищенная сеть);
- порядок предоставления доступа к ИС Защищенной сети;
- порядок организации защищенного межсетевого взаимодействия;
- порядок разрешения конфликтных ситуаций.

3.4. Общими требованиями к оборудованию и ПО рабочих мест, подключаемых к Защищенной сети в качестве узлов ViPNet, являются:

- использование лицензионной операционной системы Windows, версии не ниже 8.1 (32/64-разрядной);
- установка лицензионного сертифицированного антивирусного ПО;
- реализация системы аутентификации и разграничения доступа пользователей.

4. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ УЧАСТНИКОВ К ЗАЩИЩЕННОЙ СЕТИ

4.1. Организация подключения Участников к Защищенной сети включает в себя следующие стадии:

- заявительная стадия;
- стадия рассмотрения заявления;
- закупка ПО ViPNet [Клиент], средств защиты информации (далее - СЗИ) (для Претендентов, включенных в муниципальное задание МАУ «ЦМИРиТ» осуществляет учреждение) сторонние организации осуществляют закупку самостоятельно;
- формирование и передача ключевой информации Участнику;
- подключение и настройка Узла ViPNet Участника.

4.2. Заявительная стадия.

Претендент, желающий подключиться к Защищенной сети, направляет в адрес МАУ «ЦМИРиТ» оформленное на бланке организации письменное заявление **(Приложение 1)** о намерении подключиться к Защищенной сети. Допускается подача заявления в электронном виде (в виде цветного скана документа),

направленного на официальный электронный адрес МАУ «ЦМИРиТ» (cmirit@cherepovetscity.ru), либо через систему ITSM МАУ «ЦМИРиТ» (при ее наличии у Претендента).

При запросе доступа к ИС Участников, Претендент прикладывает к заявлению документ(ы), подтверждающий требование или согласие правообладателя ИС (далее - Правообладатель) на предоставление Претенденту доступа к данной ИС.

4.2.1. В заявлении должна содержаться следующая информация:

- количество подключаемых Узлов ViPNet;
- перечень Участников, с которыми необходима организация защищенного обмена Претендента;
- Данные подключения (URL, ip-адрес) к информационных системам, к которым необходимо организовать доступ Претендента;
- ФИО и контактный телефон лица ответственного за подключение Претендента.

4.3. Стадия рассмотрения заявления.

4.3.1. Руководство МАУ «ЦМИРиТ» рассматривает поступившие заявления о намерении подключиться к Защищенной сети в течение 5-х рабочих дней со дня получения каждого поступившего заявления.

4.3.2. При рассмотрении заявления оцениваются основания для подключения Претендента к Защищенной сети, а также техническая возможность организации направлений связи и доступа к информационным системам.

4.3.3. Результат рассмотрения заявления направляется официальным письмом, отражающий принятое решение, в письменной форме в почтовый адрес Претендента, либо по электронной почте, указанной в заявке Претендента, или через систему ITSM МАУ «ЦМИРиТ», со сканом письма во вложении, в течение 3-х рабочих дней со дня принятия указанного решения.

В случае положительного решения, в письме могут быть указаны ограничения, накладываемые на Участников Защищенной сети.

4.3.4. Владелец Защищенной сети имеет право отказать Претенденту в подключении к Защищенной сети.

4.4. Закупка ПО ViPNet [Клиент] и СЗИ Претендентом.

4.4.1. Приобретение ПО ViPNet [Клиент] и СЗИ, до рассмотрения заявления о намерении подключиться к Защищенной сети, не являются основанием и гарантией подключения Претендента к Защищенной сети.

4.4.2. В случае принятия положительного решения о подключении к Защищенной сети, Претендент самостоятельно приобретает ПО ViPNet [Клиент] и СЗИ (кроме Претендентов, включенных в муниципальное задание МАУ «ЦМИРиТ»).

4.4.3. При заключении договора о покупке ПО ViPNet [Клиент] Претендент указывает в договоре номер Защищенной сети для подключения - **2317**.

4.4.4. В случае принятия положительного решения о подключении к Защищенной сети, Претендент:

- заключает договор с МАУ «ЦМИРиТ» (для Претендентов, включенных в муниципальное задание МАУ «ЦМИРиТ», договор не требуется) на обслуживание узлов ViPNet;

- назначает приказом Ответственного пользователя СКЗИ **(Приложение 2)**;

- организует работу по подготовке документации, рабочих мест и пользователей к работе с СКЗИ, в соответствии с требованиями руководящих документов, указанных в пункте 3.1 настоящего Регламента.

4.4.5. Подключение Претендента к Защищенной сети осуществляется Администратором СКЗИ ОКЗ после получения регистрационных файлов от производителя или представителя производителя ПО.

4.4.6. Администратор СКЗИ ОКЗ уведомляет Претендента о получении регистрационных файлов.

4.5. Формирование и передача ключевой информации.

4.5.1. Ответственный пользователь СКЗИ Претендента, после получения информации о поступлении регистрационных файлов, формирует и направляет в ОКЗ МАУ «ЦМИРиТ» заявку на подключение **(Приложение 3)**. Заявка направляется в электронной форме (в виде цветного скана документа), на электронный адрес ОКЗ МАУ «ЦМИРиТ» (пункт 2.5), или через систему ITSM МАУ «ЦМИРиТ» (при ее наличии у Претендента).

4.5.2. В течение 3-х рабочих дней со дня получения от Претендента заявки на подключение Администратор СКЗИ ОКЗ:

- производит регистрацию узлов и Пользователей в Центре управления сетью;

- организовывает направления связи между Узлами, в соответствии с заявкой на подключение;

- формирует дистрибутивы ключей для узлов вместе с паролем доступа к нему;

- по завершению обозначенных работ уведомляет об этом Претендента.

4.5.3. Претендент для получения дистрибутива ключей и пароля доступа к нему должен предоставить в адрес МАУ «ЦМИРиТ»:

- копию приказа о назначении Ответственного пользователя СКЗИ;

- копию договора (для Претендентов, включенных в муниципальное задание копия договора не требуется) на приобретенное ПО ViPNet [Клиент];

- носитель информации для записи дистрибутивов ключей.

4.5.4. Направить к Администратору СКЗИ Ответственного пользователя СКЗИ с доверенностью, изготовленной на бланке организации, за подписью и печатью руководителя или иного уполномоченного лица, на получение дистрибутива ключей **(Приложение 4)**.

4.5.5. Факт выдачи дистрибутива ключей Ответственному пользователю СКЗИ Претендента, заносится Администратором СКЗИ ОКЗ в Журнал учета выдачи ключевых документов **(Приложение 5)**.

4.5.6. Для получения доступа к ИС, Претендент должен обеспечить выполнение требований по информационной безопасности (уточняются у администратора ИС), предусмотренных эксплуатационной документацией на соответствующую ИС. Претендент самостоятельно приобретает (кроме Претендентов, включенных в муниципальное задание МАУ «ЦМИРиТ») устанавливает (кроме Претендентов, у которых заключен договор на Техническую поддержку с МАУ «ЦМИРиТ») необходимые СЗИ и предоставляет в адрес МАУ «ЦМИРиТ» подтверждение установки приобретенных СЗИ (скриншот). Состав СЗИ предварительно согласовывается с МАУ «ЦМИРиТ».

4.6. Подключение и настройка Узла ViPNet Участника.

4.6.1. Подключение Узла ViPNet Участника к Защищенной виртуальной сети и его настройка может быть выполнена:

- самостоятельно Ответственным пользователем СКЗИ Участника в соответствии с технической документацией на ПО ViPNet [Клиент];
- Администратором ОКЗ удаленно;
- Администратором ОКЗ на рабочем месте Участника.

4.6.2. В случае самостоятельного подключения Узла ViPNet Участником, Ответственный пользователь СКЗИ должно действовать в соответствии с Руководством пользователя на ПО ViPNet [Клиент]. В случае правильной установки ПО и успешного ввода дистрибутива ключей, подключение к защищенной сети произойдет автоматически.

4.6.3. Для удаленного подключения Узла ViPNet Администратором СКЗИ ОКЗ, Ответственный пользователь СКЗИ Участника согласует с Администратором СКЗИ ОКЗ дату и время выполнения работ, тип программы удаленного доступа, а также обеспечивает готовность рабочего места и программы удаленного доступа для выполнения работ.

4.6.4. В случае невозможности организации удаленного доступа Администратора СКЗИ ОКЗ к рабочему месту Участника, либо при возникновении неустранимых технических проблем с удаленной установкой, Ответственный пользователь СКЗИ Участника согласует с Администратором СКЗИ ОКЗ время и дату выполнения работ по подключению непосредственно на рабочем месте и в назначенный срок лично предоставляет Узел ViPNet Администратору СКЗИ ОКЗ для выполнения работ по подключению.

5. ПОРЯДОК ИЗМЕНЕНИЯ НАПРАВЛЕНИЙ СВЯЗИ И/ИЛИ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ ЗАЩИЩЁННОЙ СЕТИ

5.1. Порядок изменения направлений связи и/или предоставление доступа к информационным системам включает в себя следующие стадии:

- заявительная стадия;
- стадия рассмотрения заявления;
- формирование и передача ключевой информации;

5.2. Заявительная стадия.

5.2.1. Для получения доступа к информационным системам Участников, Претендент должен предоставить ОКЗ в адрес МАУ «ЦМИРиТ» документ, подтверждающий согласие правообладателя информационной системы (далее - Правообладатель) на предоставление доступа к информационной системе.

5.2.2. Участник, желающий изменить направление связей и/или получить доступ к информационным системам Защищенной сети направляет в адрес ОКЗ МАУ «ЦМИРиТ» заявку за подписью Ответственного пользователя СКЗИ **(Приложение 6)**. Способы отправки заявки указаны в п.4.5.1.

Заявка должна быть согласована с Правообладателем ИС, или к ней должен быть приложен документ, подтверждающий требование/согласие Правообладателя ИС на предоставление доступа Участнику к данной ИС.

5.2.3. При заполнении заявки следует указывать все необходимые на данный момент направления связи и все информационные системы Защищенной сети, к которым необходим доступ (**URL, ip-адрес**).

5.3. Рассмотрение заявления.

5.3.1. ОКЗ в течение 5-ти рабочих дней со дня получения рассматривает заявление об изменении направлений связи и/или организации доступа к информационным системам.

5.3.2. Решение об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, направляется в письменной форме в адрес Претендента или по электронной почте, указанной в заявке или через систему ITSM МАУ «ЦМИРиТ» в течение 3-х рабочих дней со дня принятия указанного решения.

5.3.3. ОКЗ имеет право отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, по следующим причинам:

- отсутствие технической возможности организации направления связи;
- отказ Правообладателя ИС в предоставлении доступа.

5.3.4. Решение об отказе в изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, направляется в письменной форме в адрес Претендента или по электронной почте, указанной в заявке или через систему ITSM МАУ «ЦМИРиТ» в течение 3-х рабочих дней со дня принятия указанного решения.

5.4. Формирование и передача ключевой информации.

5.4.1. В течение 5 рабочих дней со дня уведомления Участника о принятии решения об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети Администратор СКЗИ ОКЗ вносит следующие изменения.

- вносит изменения в направления связей между Узлами, в соответствии с заявлением;
- формирует необходимую справочную и ключевую информацию;

- через Центр управления сетью направляет справочную и ключевую информацию на соответствующие Узлы Участника;

- по завершению обозначенных работ уведомляет об этом Участника.

5.4.2. При поступлении на Узел ViPNet новая ключевая информация автоматически обновляет существующую ключевую информацию.

6. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СЕТЯМИ VIPNET

6.1. Организация межсетевого взаимодействия с другими сетями ViPNet включает в себя следующие стадии:

- заявительная стадия;

- рассмотрение заявки;

- формирование и передача ключевой информации;

6.2. Заявительная стадия.

6.2.1. Для организации межсетевого взаимодействия между Защищенной сетью и сторонней сетью ViPNet, Администратор СКЗИ Защищенной сети или администратор сторонней ViPNet сети готовят соглашение об межсетевом взаимодействии, в котором информируют другую сторону о необходимости организации межсетевого взаимодействия с указанием контактов Ответственных лиц за организацию межсетевого взаимодействия.

6.3. Рассмотрение заявления.

6.3.1. Владелец Защищенной сети в течение 5-ти рабочих дней со дня получения информационного заявления проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

6.3.2. Решение об организации межсетевого взаимодействия, направляется в письменной форме, в адрес организации инициирующей данное межсетевое взаимодействие или по электронной почте указанной письме в течение 3-х рабочих дней со дня принятия указанного решения.

6.3.3. Владелец Защищенной сети имеет право отказать в организации межсетевого взаимодействия, по следующим причинам:

- отсутствие технической возможности установления межсетевого взаимодействия или организации направления связи;

- отказ Владельца защищенной виртуальной сети в установлении межсетевого взаимодействия;

- отказ Правообладателя информационной системы в предоставлении доступа.

6.3.4. Решение об отказе в организации межсетевого взаимодействия направляется в письменной форме, в адрес организации инициирующей данное межсетевое взаимодействие или по электронной почте, указанной в информационном письме в течение 3-х рабочих дней со дня принятия указанного решения.

6.4. Формирование и передача ключевой информации.

6.4.1. В случае принятия решения об организации межсетевого взаимодействия, Администратор СКЗИ и администратор сторонней сети ViPNet, в соответствии с «Руководством администратора ViPNet Administrator [Центр управлению сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр] » производят формирование необходимой адресной и ключевой информации - формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочную информацию), включая корневые сертификаты для каждой их сетей.

6.4.2. Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие Центры управления сетей (далее - ЦУС), с которыми должно осуществляться межсетевое взаимодействие.

6.4.3. Во всех ЦУС в соответствии с «Руководством администратора. ViPNet Administrator [Центр управлению сетью] » и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр] » производится ввод и обработка (импорт) полученных из других ЦУС данных (начального экспорта), установление связей своих Узлов с Узлами ЦУС, предоставившими информацию (ответный экспорт) для ЦУС, приславших первичную информацию, включая свои сертификаты.

6.4.4. Ответная информация (ответный экспорт) доверенным способом передается в соответствующие ЦУС, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого взаимодействия между ЦУС, в дальнейшем обмен данными между ними производится в автоматическом режиме.

6.4.5. Сформированная ключевая и справочная информация через ЦУС отправляется на узлы, участвующие в межсетевом взаимодействии.

6.4.6. После завершения процедуры организации межсетевого взаимодействия между Защищенной сетью и сторонней Защищенной сетью ViPNet, подписывается Протокол установления межсетевого взаимодействия (**Приложение № 7**).

6.5. Организация направлений связи между Узлами сторонней сети ViPNet и Узлами Защищенной сети, осуществляется в соответствии с разделом 4 настоящего Регламента.

6.6. При каждой модификации межсетевого взаимодействия Администратор СКЗИ ОКЗ вносит соответствующие записи в Журнал изменений межсетевого взаимодействия (**Приложение 8**).

7. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ ПЛАНОВОЙ СМЕНЫ МЕЖСЕТЕВОГО МАСТЕР-КЛЮЧА.

7.1. Порядок организации межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа предполагает выполнение ряда технологических и организационных мероприятий.

7.2. Предварительные организационные мероприятия.

Перед осуществлением плановой смены межсетевого мастер-ключа, Администратор СКЗИ и администратор сторонней сети ViPNet, должны:

- выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;

- в случае использования симметричного мастер-ключа выбирается сеть, в которой будет создан новый межсетевой мастер-ключ;

- выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для Узлов сетей.

7.3. Формирование нового межсетевого мастер-ключа.

Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр] ».

7.4. Процедура создания экспорта и приема импорта мастер-ключа.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и прием импортированных данных в соответствии с «Руководством администратора ViPNet Administrator [Центр управлению сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр] ».

7.5. Межсетевое взаимодействие после смены межсетевого мастер-ключа.

После смены межсетевого мастер-ключа связь между взаимодействующими Узлами Защищенной сети и сторонней сети ViPNet возможна только после прохождения обновления ключевой информации на всех соответствующих Узлах.

7.6. Обновленная ключевая информация через ЦУС отправляется на Узлы, участвующие в межсетевом взаимодействии.

7.7. Записи в журнале изменений межсетевого взаимодействия.

После смены межсетевого мастер-ключа Администратор СКЗИ вносит соответствующие записи в Журнал изменений межсетевого взаимодействия.

8. НАЗНАЧЕНИЕ ОТВЕТСТВЕННЫХ ЛИЦ

8.1. Назначение Руководителя ОКЗ осуществляется приказом директора МАУ «ЦМИРиТ».

8.1.1. Исполнение функций ОКЗ осуществляется сектором по безопасности и защите информации МАУ «ЦМИРиТ».

8.1.2. Руководитель ОКЗ в своей деятельности руководствуется законодательством Российской федерации в области защиты информации, а также нормативными актами, регулирующими вопросы в области криптографической защиты информации.

8.2. Назначение Администратора СКЗИ осуществляется приказом директора МАУ «ЦМИРиТ».

8.2.1. Администратор СКЗИ в своей деятельности руководствуется законодательством Российской федерации в области защиты информации, а также

нормативными актами, регулирующими вопросы в области криптографической защиты информации.

8.3 Назначение Ответственного пользователя СКЗИ Участника осуществляется приказом его руководителя.

8.3.1 Ответственный пользователь СКЗИ Участника руководствуется законодательством Российской федерации в области защиты информации, а также нормативными актами, регулирующими вопросы в области криптографической защиты информации.

8.4. В случае смены сотрудника, на которого возложены функции Ответственного пользователя СКЗИ, Участник Защищенной сети обязан в течение 2-х рабочих дней известить об этом ОКЗ Защищенной сети VipNet 2317 МАУ «ЦМИРиТ», направив копию приказа с изменениями о назначении Ответственного пользователя СКЗИ (**Приложение 2**)

9. КОМПРОМЕТАЦИЯ КЛЮЧЕЙ

9.1. К событиям компрометации, когда ключи Узла ViPNet считаются скомпрометированными, относятся следующие случаи:

- посторонним лицам мог стать доступен (стал доступен) файл ключевого дистрибутива Узла ViPNet;
- посторонним лицам мог стать доступен (стал доступен) съемный носитель ключевой информации Пользователя;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Узле ViPNet;
- на Узле отсутствовал (был отключен) модуль ViPNet [Клиент], или он устанавливался в 4-й или 5-й режим, и в локальной сети считается возможным присутствие посторонних лиц;
- прекращение полномочий Ответственного пользователя СКЗИ Участника Защищенной сети, в соответствии с приказом, имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора (договора возмездного оказания услуг).

9.2. При возникновении подозрений об известности посторонним лицам пароля доступа Пользователя при старте модуля ViPNet [Клиент], при условии, что доступ к Узлу ViPNet посторонних лиц был невозможен, Администратору СКЗИ следует сменить пароль и разрешить Пользователям продолжить работу.

9.3. При возникновении подозрений об известности посторонним лицам пароля доступа Пользователя при старте модуля ViPNet [Клиент], при условии, что доступ к Узлу посторонних лиц был возможен, ключи считаются скомпрометированными.

9.4. К событиям, требующим проведения расследования и принятия решения на предмет компрометации ключевой информации, относится возникновение подозрений в утечке информации при ее передаче посредством Защищенной сети.

9.5. В случае прекращения полномочий Пользователя, ключи данного Пользователя считаются скомпрометированными.

9.6. В случае прекращения полномочий Ответственного пользователя СКЗИ участника Защищенной сети, ключевая информация всех Пользователей Участника считается скомпрометированной.

9.7. В случае наступления любого из событий, связанных с компрометацией ключевой информации, Пользователь немедленно прекращает связь с другими Узлами ViPNet и сообщает о факте компрометации своему Ответственному пользователя СКЗИ Участника Защищенной сети.

9.8. Ответственный пользователь СКЗИ Участника Защищенной виртуальной сети доводит информацию о факте компрометации (или предполагаемом факте компрометации) до ОКЗ.

9.9. Администратор СКЗИ при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

- в ПО ViPNet [Администратор] объявить ключи Узла скомпрометированными и создать средствами ПО справочники связей при компрометации с необходимой информацией;
- оповестить о факте компрометации ключей всех Пользователей, связанных с Пользователем, ключевая информация которого была скомпрометирована;
- сформировать средствами ПО ViPNet [Администратор] новую ключевую информацию.
- произвести рассылку сформированных обновлений ключей на Узлы Защищенной сети.

Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Узел по любым каналам связи;

- После прохождения обновления ключей возобновить работу на скомпрометированном Узле.

10. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ КОПРОМЕТАЦИИ КЛЮЧЕЙ

10.1. Компрометация ключей Администратора.

При наступлении любого из перечисленных в п.9.1. настоящего Регламента событий, Узел Администратор, **должен немедленно прекратить работу** на своем Узле и сообщить о факте компрометации Администратору сторонней сети.

10.1.1. Администратор сторонней сети ViPNet при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

- в ПО ViPNet [Администратор] объявить ключи Узла скомпрометированными и создать, средствами ПО, справочники связей при компрометации с необходимой информацией;

- оповестить о факте компрометации ключей всех Пользователей, связанных со сторонней сетью ViPNet, ключевая информация которой была скомпрометирована;

- найти и устранить причину повлекшей компрометацию ключей Узла Администратора.

- сформировать средствами ПО ViPNet [Администратор] новую ключевую информацию.

- произвести рассылку сформированных обновлений ключей на Узлы Защищенной сети;

- сформировать и отправить импорт для сети ViPNet, с Узлами которой взаимодействовал скомпрометированный Узел.

- После прохождения обновления ключей возобновить работу на скомпрометированном Узле.

10.1.2. Администратор сторонней сети ViPNet, Пользователи которой взаимодействовали с Пользователем, ключи которого скомпрометированы, после приема и обработки импорта создает новую ключевую информацию своим Пользователям.

Возобновление межсетевого взаимодействия возможно только после прохождения обновления ключевой информации на всех взаимодействующих Узлах.

10.2. Внеплановая смена межсетевого мастер-ключа.

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер-ключа, на котором происходит организация межсетевого взаимодействия.

10.2.1. В случае компрометации симметричного межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при защищенном межсетевом взаимодействии, в таком случае межсетевое взаимодействие должно **быть немедленно остановлено**.

10.2.2. Для восстановления работы межсетевого взаимодействия необходимо произвести технологические и организационные мероприятия, описанные в разделе 7 «Порядок организации защищенного межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа».

10.2.3. При компрометации ключей Администратор СКЗИ вносит соответствующие записи в Журнал изменений межсетевого взаимодействия.

11. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

11.1. Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения Участниками электронных документов и/или получением доступа к информационным системам других Участников Защищенной сети.

11.2. Разрешение конфликтных ситуаций осуществляется путем взаимодействия Ответственных пользователей СКЗИ Участников Защищенной сети и при участии Администратора СКЗИ.

11.3. В случае необходимости, для разрешения конфликтных ситуаций, может быть привлечен Руководитель ОКЗ.

12. ПОРЯДОК ПОЛУЧЕНИЯ ДУБЛИКАТОВ ДИСТРИБУТИВА КЛЮЧЕЙ (DST-файлов)

12.1. Ответственный пользователь СКЗИ Участника направляет обоснованную заявку в ОКЗ МАУ «ЦМИРиТ» на получение дубликата дистрибутива ключей **(Приложение 9).** Способы отправки заявки указаны в п. 4.5.1.

12.1.1. В случае, если изменения в Защищенной сети, повлекшие за собой неработоспособность ViPNet [Клиент] Претендента, были инициированы Владельцем или Администратором СКЗИ, подача заявки на получение дубликата дистрибутива ключей не требуется.

В этом случае Претендент должен уведомить Администратора СКЗИ о неработоспособности, написав письмо на электронную почту bizi@cherepovetscity.ru с указанием наименования Узла, который потерял доступ к Защищенной сети, а также способа передачи дубликата дистрибутива ключей, согласно пункту

12.2. Если на момент внесения изменений в Защищенной сети ViPNet [Клиент] Претендента был неактивен более 6 месяцев, то Претендент направляет заявку в ОКЗ на получение дубликата дистрибутива ключей.

12.3. В течение 1 рабочего дня с момента получения от Претендента заявки на получение дубликата дистрибутива ключей Администратор СКЗИ:

- формирует дубликат дистрибутива ключей для Узлов вместе с паролем доступа к нему;
- по завершению обозначенных работ уведомляет об этом Претендента.

12.4. Передача дубликата дистрибутива ключей производится:

- по деловой почте ViPNet [Клиент] при рабочем канале (когда доступен Координатор 2317).
- лично сотрудником Претендента с доверенностью на получения дубликата дистрибутива ключей.

Заявки Претендента и реквизиты выданных дубликатов дистрибутивов ключей регистрируются в Журнале учета и выдачи дистрибутивов Ключей (**Приложение 5**).

13. ОТВЕТСТВЕННОСТЬ

Владелец защищенная сети не несет ответственности в случае нарушения Участниками Защищенной сети положений настоящего Регламента.

Участник Защищенной сети несет материальную ответственность за ненадлежащую эксплуатацию физических носителей информации, сохранение в

тайне ключевой информации, владельцем которой он является, и своевременность оповещения Администратора СКЗИ о возможной компрометации ключевой информации.

14. ПРАВА

14.1. Права ОКЗ.

ОКЗ защищенной виртуальной сети имеет право:

14.1.1. Отказать Претенденту в подключении к Защищенной сети, по причинам, указанным в пункте 4.4.1 данного регламента.

14.1.2. Отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, по причинам, указанным в пункте 5.3.3 данного регламента.

14.1.3. Отказать в организации межсетевого взаимодействия, по причинам, указанным в пункте 6.3.3 данного регламента.

14.1.4. Отключить Участника от Защищенной сети в случае нарушения положений Регламента.

14.2. Права Претендентов и Участников Защищенной сети.

14.2.1. Обратиться к ОКЗ с заявлением о подключении к Защищенной сети.

14.2.2. Обратиться к ОКЗ защищенной сети с заявлением об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети.

14.2.3. Обратиться к ОКЗ защищенной сети с заявлением об организации межсетевого взаимодействия.

15. ОБЯЗАТЕЛЬСТВА МАУ «ЦМИРиТ»

Муниципального автономное учреждение «Центр муниципальных информационных ресурсов у технологий» обязано поддерживать уровень защиты информации в Защищенной виртуальной сети в соответствии с требованиями законодательства Российской Федерации в области информационной безопасности.