



Администрация муниципального округа город Мончегорск
с подведомственной территорией Мурманской области
(АДМИНИСТРАЦИЯ города МОНЧЕГОРСКА)

РАСПОРЯЖЕНИЕ

18.02.2022

№42-р

Мончегорск

Об утверждении регламента подключения участников к виртуальной защищённой сети администрации города Мончегорска

В целях обеспечения защиты информации от несанкционированного доступа в соответствии с требованиями федеральных законов от 27.07.2006 № 152-ФЗ "О персональных данных", от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", приказов ФСБ России от 09.02.2005 № 66 "Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)", от 10.07.2014 № 378 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

Утвердить прилагаемый Регламент по подключению участников к виртуальной защищенной сети администрации города Мончегорска.

Глава администрации города

В.И. Садчиков

Утвержден
распоряжением администрации
города Мончегорска
от 18.02.2022 №42-р

РЕГЛАМЕНТ
подключения участников к виртуальной защищённой сети
администрации города Мончегорска

Мончегорск
2022 год

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ViPNet Администратор	программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищенной сетью, организованной с использованием технологии "ViPNet".
ViPNet Клиент	программный комплекс, реализующее на рабочем месте пользователя функции VPN-клиента, персонального сетевого экрана.
ViPNet Координатор	программное обеспечение или программно-аппаратный комплекс, выполняющий функцию узла виртуальной защищенной сети, организованной с использованием технологии "ViPNet".
VPN (Virtual Private Network)	обобщенное название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
Абонентский пункт	рабочая станция (персональный компьютер) с установленным программным обеспечением "ViPNet Клиент", входящий в состав виртуальной защищенной сети администрации города Мончегорска.
Администратор виртуальной защищенной сети (Администратор)	юридическое лицо, на которое возложены функции организационно-технического сопровождения работы защищенной сети и ее развития, координации действий Участников и обладающее соответствующей разрешительной (лицензионной) базой в соответствии с действующим законодательством.
Оператор информационных систем	участник системы, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством.
Дистрибутив ключей	файл с расширением .dst, создаваемый в программе "ViPNet Администратор" для каждого пользователя сетевого узла "ViPNet". Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы "ViPNet" на сетевом узле.
Доверенный способ передачи информации	способ передачи информации обеспечивающий требуемые уровни безопасности и конфиденциальности.
Виртуальная защищенная сеть (ВЗС администрации города)	виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий межсетевого экранирования и VPN, реализованная сертифицированными в установленном порядке средствами защиты информации
Информационная система	совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий, технических средств и персонала.
Администрация города	Администрация города Мончегорска.
Компрометация защищаемой (ключевой) информации	факт доступа (подозрение в факте доступа) посторонних лиц к защищаемой (ключевой) информации.

Компонент ВЗС администрации города (Компонент)	сетевой узел, обеспечивающий функционирование виртуальной защищенной сетью администрации города, и представляющий собой программное обеспечение, программно-аппаратный комплекс "ViPNet".
Контролируемая зона	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных, технических и иных материальных средств.
Несанкционированный доступ	доступ к закрытой (ограниченной в законном порядке) информации посторонних лиц, не имеющих разрешения на доступ к такой информации.
Ответственный пользователь Участника ВЗС администрации города (Ответственный пользователь Участника)	контактное (должностное) лицо Участника, осуществляющее организацию подключения и ответственное за взаимодействие с Администратором виртуальной защищенной сети администрации города.
Пользователь Участника ВЗС администрации города (Пользователь Участника)	должностное лицо Участника, использующее для выполнения своих служебных обязанностей доступ к информационным системам и ресурсам, входящим в состав виртуальной защищенной сети администрации города.
Претендент	юридическое лицо, имеющее намерение подключиться к ВЗС администрации города.
Резервный набор персональных ключей пользователя	предназначен для обновления ключевой информации в случае смены мастер-ключа персональных ключей или в случае перехода на новый вариант персонального ключа пользователя.
Технология ViPNet	технология, предназначенная для построения виртуальных защищенных сетей путем использования системы персональных и межсетевых экранов на защищаемых компонентах распределенной сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами.
Участник ВЗС администрации города (Участник)	юридическое лицо (структурные подразделения администрации города Мончегорска и её отраслевые (функциональные) органы), являющееся оператором информации, формирующейся и обрабатываемой в процессе деятельности отраслевых (функциональных) органов администрации города); юридические и физические лица, осуществляющие обслуживание информационных систем и ресурсов Операторов информационных систем на договорной основе и подключенные к виртуальной защищенной сети администрации города в установленном в настоящем Регламенте порядке.
Центр управления сетью	аппаратные и/или программные средства для мониторинга, конфигурирования и управления Компонентами виртуальной защищенной сети администрации города.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Регламент подключения к защищенной виртуальной сети администрации города Мончегорска (далее по тексту - Регламент) разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации:

- Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";

- 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 ФСБ России от 10.07.2014 № 378 "Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности";

- иными нормативно-правовыми и подзаконными актами Российской Федерации, рекомендательными документами государственных регуляторов в области защиты информации и информационной безопасности.

1.2. Настоящий Регламент определяет и устанавливает:

1.2.1. Состав и порядок функционирования виртуальной защищенной сети администрации города (далее по тексту – ВЗС администрации).

1.2.2. Порядок подключения Претендентов и Участников ВЗС администрации.

1.2.3. Порядок организации защищённого межсетевое взаимодействия.

1.2.4. Требования, предъявляемые при работе в ВЗС администрации.

1.3. ВЗС администрации города реализована с использованием программно-аппаратных комплексов и программного обеспечения, основанного на технологии "ViPNet".

1.4. Администрирование и техническое сопровождение ВЗС администрации должно осуществляться организацией (юридическим лицом), располагающим соответствующей разрешительной (лицензионной) базой в соответствии с действующим законодательством РФ в области информационной безопасности и технической защиты конфиденциальной информации (в том числе криптографическими методами), а также обладающая подтвержденным производителем и правообладателем (АО "ИнфоТеКС") документально правом на техническую поддержку средств защиты информации с использованием технологии "ViPNet".

1.5. В настоящий Регламент могут быть внесены изменения, связанные с развитием (изменением) технологии обработки информации Компонент ВЗС администрации, изменением её структуры, а также изменениями в действующем законодательстве РФ в области информационной безопасности и технической защиты информации (в том числе криптографическими методами).

2. НАЗНАЧЕНИЕ ВЗС АДМИНИСТРАЦИИ ГОРОДА

2.1. Целью создания ВЗС администрации является обеспечение информационной безопасности при передаче информации между Участниками ВЗС администрации, в том числе информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, с использованием публичных и выделенных каналов связи путем организации виртуальной сети.

2.2. ВЗС администрации обеспечивает:

2.2.1. Предотвращение несанкционированного доступа к информации, в том числе информации ограниченного доступа и (или) передачи ее лицам, не имеющим права на доступ к информации.

2.2.2. Защиту конфиденциальной информации, иной охраняемой законодательством Российской Федерации информации, в том числе персональных данных, при взаимодействии информационных систем или ее отдельных сегментов с иными информационными системами и информационно - телекоммуникационными сетями.

2.3. ВЗС администрации создана на основе информационно-вычислительной сети администрации города Мончегорска (далее по тексту – ИВС администрации), включающей в себя локальную вычислительную сеть здания администрации города, являющуюся узловым (центральным) Компонентом системы, и подключенные к ней в установленном порядке локальные вычислительные сети иных зданий, в которых размещаются отраслевые (функциональные) органы администрации города. Объединение в единую ИВС администрации осуществляется с использованием волоконно-оптических линий связи.

3. СТРУКТУРА И СОСТАВ ВЗС АДМИНИСТРАЦИИ ГОРОДА

3.1. ВЗС администрации представляет собой территориально распределенную информационно-телекоммуникационную сеть, объединяющую Компоненты ВЗС администрации.

3.2. Предоставление доступа Участнику к информационным системам и ресурсам, размещенным на оборудовании, входящем в состав ИВС администрации, осуществляется с использованием Компонентов ВЗС администрации.

3.3. Центр управления ВЗС администрации физически расположен в локальной вычислительной сети здания администрации города Мончегорска.

3.4. Взаимодействие Компонентов ВЗС администрации осуществляется по каналам связи, используемыми Участниками.

3.5. Программное обеспечение, обеспечивающее функционирование ВЗС администрации, состоит из Компонентов: "ViPNet Администратор", "ViPNet Координатор", а также "ViPNet Клиент", устанавливаемый на оборудовании Участников.

3.6. Участник обязан обеспечить информационную безопасность и техническую защиту информации каждого подключаемого Компонента в соответствии с законодательством Российской Федерации, а также технической и эксплуатационной документацией на Компоненты.

3.7. Компоненты, устанавливаемые у Участников:

3.7.1. Должны находиться в пределах контролируемой зоны Участников, быть в работоспособном состоянии, доступными для других Участников при защищенном и межсетевом взаимодействии, за исключением времени проведения ремонтных и планово-профилактических работ, осуществляемых Администратором ВЗС администрации.

3.7.2. Иметь действующие сертификаты соответствия средств защиты информации по требованиям безопасности информации и введены в эксплуатацию в соответствии с технической и эксплуатационной документацией на Компоненты.

3.8. Абонентские пункты Участников должны быть обеспечены сертифицированными и имеющим действующий сертификат соответствия средствами защиты информации о несанкционированного доступа (СЗИ от НСД).

3.9. Абонентские пункты Участников должны быть обеспечены средствами антивирусной защиты информации имеющие регулярный доступ и получения обновлений антивирусных баз.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ И ОТКЛЮЧЕНИЯ УЧАСТНИКОВ К/ОТ ВЗС АДМИНИСТРАЦИИ ГОРОДА

4.1. Организация подключения новых Участников включает в себя следующие этапы:

4.1.1. Подача Претендентом комплекта документов на подключение к ВЗС администрации.

4.1.2. Рассмотрение комплекта документов, информирование Претендента о результатах рассмотрения.

4.1.3. Приобретение Участником программного обеспечения.

4.1.4. Формирование и передача дистрибутива ключевой информации Участнику.

4.2. Подача Претендентом комплекта документов на подключение к ВЗС администрации:

4.2.1. Претендент формирует и направляет Администратору комплект документов, подписанный руководителем Претендента, о намерении подключиться к ВЗС администрации, с указанием цели подключения, списка пользователей, перечня информационных ресурсов, с которыми необходима организация защищённого информационного обмена.

4.2.2. В комплект документов, передаваемый Претендентом входят:

- заявление на подключение к ВЗС администрации, оформленного в соответствии с Приложением № 1 к настоящему Регламенту;

- заявление на регистрацию пользователя ВЗС администрации, оформленного в соответствии с Приложением № 2 к настоящему Регламенту.

4.2.3. В заявлении на подключение должна содержаться следующая информация:

- предполагаемое количество подключаемых Абонентских пунктов;

- общий перечень Участников, с которыми необходима организация защищенного обмена;

- перечень информационных ресурсов ВЗС администрации, к которым необходимо организовать доступ;

- ФИО и контактный телефон лица, ответственного за подключение со стороны Претендента (далее по тексту – Ответственный пользователь Участника).

4.3. Рассмотрение комплекта документов.

4.3.1. Администратор в течение 3 (трех) рабочих дней со дня получения комплекта документов проводит оценку оснований для подключения Претендента к ВЗС администрации, технической возможности организации связей и доступа к информационным ресурсам, указанным в заявлении.

4.3.2. Приобретение программного обеспечения до момента рассмотрения комплекта документов о намерении подключиться к ВЗС администрации не является основанием и гарантией подключения Претендента.

4.3.3. Решение о подключении к ВЗС администрации направляется в электронной форме в адрес Претендента, указанный в заявлении на подключение. При положительном решении Претендент становится Участником.

4.3.4. В случае отрицательного результата рассмотрения комплекта документов, Администратор уведомляет Претендента об отказе в подключении к ВЗС администрации. Решение об отказе направляется в электронной форме в адрес Претендента, указанный в заявлении на подключение.

4.4. Приобретение программного обеспечения.

4.4.1. Подключение нового Участника осуществляется с использованием программного обеспечения "ViPNet". Обеспечение необходимым для подключения количеством лицензий осуществляется новым Участником самостоятельно. При оформлении документов на приобретение лицензии на программные продукты новый Участник указывает регистрационный номер ВЗС администрации "1105". Количество приобретаемых лицензий должно соответствовать количеству планируемых к подключению Абонентских пунктов нового Участника, указанных в заявительных документах.

4.4.2. Подключение Претендента к ВЗС администрации осуществляется Администратором в течение 5 (пяти) рабочих дней, с даты получения регистрационных файлов (файлов, содержащих информацию о приобретенных Претендентом лицензиях) от производителя программного обеспечения или представителя производителя программного обеспечения "ViPNet".

4.5. Формирование и передача дистрибутива ключевой информации.

4.5.1. Претендент для получения дистрибутива ключевой информации и пароля доступа к нему должен направить к Администратору Ответственного пользователя/Пользователя или иного представителя Претендента с доверенностью на получение дистрибутива ключевой информации. Доверенность представителя Претендента оформляется в соответствии с Приложением № 3 к настоящему Регламенту.

4.5.2. Факт выдачи дистрибутива ключевой информации заносится в "Журнал поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов" Администратора ВЗС администрации. В обязательном порядке для Ответственного пользователя/Пользователя или иного представителя Претендента проводится краткий инструктаж по обращению со средствами криптографической защиты информации, с фиксированием факта проведения инструктажа в журнале установленной формы, а также осуществляется выдача порядка действий при компрометации ключевой информации.

4.5.3. Повторное формирование дистрибутива ключевой информации зарегистрированного Абонентского пункта, в том числе в случаях внесения в ВЗС администрации изменений, инициированных Администратором, повлекших за собой неработоспособность Абонентского пункта Участника, производится на основании подачи Участником заявления, оформленного в соответствии с Приложением № 4 к настоящему Регламенту.

4.5.4. Формирование дистрибутива ключевой информации осуществляется Администратором в течение 5 (пяти) рабочих дней с момента получения от Участника соответствующего заявления. По завершению обозначенных работ Администратор ВЗС уведомляет об этом Участника в электронной форме на адрес, указанный в заявлении.

4.5.5. Получение дистрибутива ключевой информации производится Участником в соответствии с пунктами 4.5.1 и 4.5.2.

4.5.6. На Участника распространяются все обязанности по соблюдению требований информационной безопасности, установленные действующим законодательством в области защиты информации, технической и эксплуатационной документацией на Компоненты и настоящим Регламентом.

4.6. Участник имеет право произвести отключение от ВЗС администрации, направив Администратору соответствующее заявление, оформленное в соответствии с Приложением № 6 к настоящему Регламенту.

4.6.1. Отключение Участника от ВЗС администрации осуществляется Администратором ВЗС в течение 2 (двух) рабочих дней с момента получения от Участника соответствующего заявления.

5. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ ЗАЩИЩЕННЫМИ СЕТЯМИ

5.1. Для организации межсетевого взаимодействия (далее по тексту – МСВ) между ВЗС администрации и организацией, подключенной или владеющей сторонней сетью "ViPNet" (далее по тексту – Организация), Организация готовит информационное письмо, в котором информирует Администратора ВЗС администрации о необходимости организации информационного МСВ с указанием контактов ответственных лиц.

5.2. Администратор в течение 5 (пяти) рабочих дней со дня получения информационного письма проводит оценку оснований и технической возможности для организации МСВ.

5.3. После принятия решения об организации либо об отказе в организации МСВ Администратор в письменной форме, либо по электронной почте уведомляет о принятом решении Организацию, иницилирующую данное взаимодействие.

5.4. При положительном решении, Администратор в течение 3 (трех) рабочих дней направляет на подписание в организацию, иницилирующую данное взаимодействие, типовое Соглашение об установлении межсетевое взаимодействия, оформленное в соответствии с Приложением № 7 к настоящему Регламенту.

5.5. После подписания Соглашения об установлении МСВ, Администратор ВЗС администрации и Администратор сторонней сети "ViPNet", в соответствии с технической и эксплуатационной документацией на программное обеспечение "ViPNet", организуют МСВ с формированием необходимой справочной и ключевой информации.

5.6. Ключевая и справочная информация, необходимая для организации МСВ (начальный и ответный экспорт), передаются между соответствующими виртуальными защищенными сетями только доверенным способом.

5.7. После завершения процедуры организации МСВ, подписывается Протокол установления межсетевое взаимодействия, оформленный в соответствии с Приложением №2 к Типовому соглашению настоящего Регламента.

5.8. В случае инициативы организации МСВ со стороны Администратора ВЗС администрации в адрес Организации направляется информационное письмо, содержащее информацию о цели подключения и запрос технической возможности организации МСВ.

5.8.1. При положительном решении стороны, организующие МСВ осуществляют мероприятия в соответствии с пунктами 5.4 - 5.7 настоящего Регламента.

5.9. При организации МСВ в обязательном порядке выполняются требования по информационной безопасности и технической защите информации, предъявляемые действующим законодательством РФ, а также действующими Регламентами (Положениями) ВЗС администрации и Организации.

6. ПОРЯДОК ДЕЙСТВИЙ ПРИ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ

6.1. К событиям компрометации, когда ключи Абонентского пункта считаются скомпрометированными, относятся следующие случаи:

6.1.1. Посторонним лицам мог стать доступен (стал доступен) файл дистрибутива ключевой информации Абонентского пункта.

6.1.2. Посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте.

6.1.3. Увольнение сотрудников, являющихся Пользователями ВЗС администрации, имевших доступ к ключевой информации, а также иные события, указанные в технической и эксплуатационной документации на Компонент ВЗС администрации.

6.2. При возникновении возможности (предполагаемой возможности) нарушения конфиденциальности ключевой информации и (или) аутентификационных данных Абонентского пункта, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, ключевая информация считается скомпрометированной.

6.3. При наступлении любого из перечисленных в пункте 6.1 событий, Пользователь должен немедленно прекратить работу на Абонентском пункте и сообщить о факте компрометации (или предполагаемом факте компрометации) Ответственному пользователю или в случае отсутствия такового, напрямую Администратору ВЗС администрации.

6.4. Ответственный пользователь в кратчайшие сроки уведомляет Администратора ВЗС администрации о факте и обстоятельствах компрометации любым доступным способом: по телефону, факсу, электронной почте и т.д.

6.5. Ответственный пользователь обязан, после уведомления о компрометации (угрозе компрометации), направить в адрес Администратора ВЗС администрации, подписанное руководителем Участника и заверенное печатью Участника Уведомление о компрометации ключей Абонентского пункта, оформленное в соответствии с Приложением № 5 к настоящему Регламенту.

6.6. Администратор при получении сообщения о компрометации ключевой информации обязан в кратчайшие сроки объявить ключевую информацию данного пользователя скомпрометированной и незамедлительно создать справочники связей для компрометации с необходимой информацией.

6.7. Администратор ВЗС администрации осуществляет формирование новой ключевой информации и рассылку сформированных обновлений ключей на Абонентские пункты, а также оповещает о факте компрометации ключей всех Участников (пользователей), связанных со скомпрометированным пользователем.

6.8. Администратор ВЗС администрации формирует новую ключевую информацию для скомпрометированного Абонентского пункта:

6.9. При наличии на скомпрометированном Абонентском пункте резервного набора персональных ключей Участника (пользователя) и отсутствия факта компрометации этого набора формирует и высылает новый ключевой набор персональных ключей пользователя.

6.10. В остальных случаях обеспечивает передачу нового дистрибутива ключевой информации пользователю.

7. ФУНКЦИИ И ПОЛНОМОЧИЯ ПОЛЬЗОВАТЕЛЯ УЧАСТНИКА

7.1. Назначение Пользователей ВЗС.

7.2. Перечень работников Пользователей Участника, которым для выполнения служебных обязанностей необходим доступ в ВЗС администрации, утверждается руководителем Участника.

7.3. В случае изменения состава Пользователей, которым для выполнения служебных обязанностей необходим доступ в ВЗС администрации, Участник обязан информировать Оператора в течение 3 (трех) рабочих дней.

7.4. Пользователи должны быть ознакомлены, с правилами работы в ВЗС администрации, предусмотренными настоящим Регламентом и предупреждены о возможной ответственности за их нарушение.

7.5. Пользователь ВЗС администрации обязан:

7.5.1. Знать и соблюдать правила информационной безопасности при работе в ВЗС, определенные настоящим Регламентом, а также другими актами, регулирующими работу в ВЗС.

7.5.2. При работе в ВЗС администрации выполнять только задания, связанные со своими должностными обязанностями.

7.5.3. При выявлении вредоносных программ или признаков нештатного функционирования программного обеспечения немедленно сообщить Администратору ВЗС администрации.

7.5.4. Предоставлять свой Абонентский пункт Администратору ВЗС для контроля и осуществления административных действий.

7.5.5. Обеспечивать безопасность хранения ключевой информации и (или) пароля.

7.6. Участникам (пользователям) ВЗС администрации запрещается:

7.6.1. Оставлять свой Абонентский пункт во включенном состоянии без контроля с незаблокированной учетной записью (устройствами ввода и отображения информации).

7.6.2. Допускать к подключенному в ВЗС администрации Абонентскому пункту посторонних лиц.

7.6.3. Самостоятельно проводить изменения в настройках Абонентского пункта.

7.6.4. Передавать пароли и ключевую информацию третьим лицам, а также размещать их в местах, доступных посторонним лицам.

7.7. Участник (пользователь) ВЗС администрации имеет право:

7.7.1. Пользоваться информационными системами, ресурсами и сервисами ВЗС администрации в рамках предоставленных ему полномочий.

7.7.2. Обращаться к непосредственному руководителю для решения вопросов использования информационных систем Участниками (пользователями).

7.7.3. Соблюдать конфиденциальность информации, полученной в связи с выполнением своих должностных обязанностей.

7.8. Пользователь ВЗС администрации несет ответственность:

7.8.1. За невыполнение требований настоящего Регламента, а также других актов, регулирующих работу ВЗС администрации.

7.8.2. За неправомерное использование информации, циркулирующей в ВЗС, к которой Пользователь Участник ВЗС администрации получает доступ в связи с выполнением своих должностных обязанностей.

7.9. Ответственность за допуск Пользователя Участника к работе в ВЗС администрации и предоставляемые ему полномочия несет руководитель Пользователя Участника, принявший решение о подключении Пользователя к ВЗС.

8. ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ

8.1. Технические мероприятия по обслуживанию Компонентов ВЗС администрации организуются Администратором ВЗС администрации.

8.2. В случае возникновения производственной необходимости проведения ремонтных и планово-профилактических работ доступ к ВЗС администрации или ее отдельным Компонентам может быть закрыт.

8.3. О проведении плановых работ (кроме аварийных и иных форс-мажорных ситуациях) Администратор уведомляет всех Участников ВЗС администрации не менее чем за 24 часа до намеченного срока начала работ.

9. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

9.1. Возникновение конфликтных ситуаций может быть связано с получением доступа к информационным ресурсам других Участников.

9.2. Разрешение конфликтных ситуаций осуществляется путем взаимодействия Пользователей Участников, у которых возникли претензии.

9.3. В случае необходимости, для разрешения конфликтных ситуаций может быть привлечен Администратор ВЗС администрации.

10. Внесение изменений и дополнений в Регламент

10.1. Внесение изменений и дополнений в Регламент осуществляется Администратором ВЗС администрации в одностороннем порядке.

10.2. Все приложения, изменения и дополнения к Регламенту являются его составной и неотъемлемой частью.

Приложение № 1
к Регламенту подключения
к виртуальной защищённой сети
администрации города Мончегорска

*(Оформляется на бланке
Организации-заявителя)*

Главе администрации
города Мончегорска

Садчикову В.И.

Заявление о подключении к виртуальной
защищенной сети администрации города Мончегорска

В соответствии с

_____ *(договор об электронном обмене, договор присоединения к информационной системе, обеспечение технической поддержки системы и т.п.)*

прошу Вас рассмотреть запрос на подключение _____
(наименование организации)

к виртуальной защищенной сети администрации города Мончегорска "ViPNet" № 1105.

Перечень информационных систем, к которым необходим доступ: _____
(наименование ИС)

Предполагаемое число подключаемых Абонентских пунктов: _____
(количество рабочих мест)

Лицо, ответственное за подключение, контактный телефон и адрес электронной почты:

(ФИО, должность, контактные данные)

(Должность руководителя)

(Подпись)

(Инициалы/Фамилия)

М.П.

Приложение № 2
к Регламенту подключения
к виртуальной защищенной сети
администрации города Мончегорска

ЗАЯВЛЕНИЕ
на регистрацию Пользователя Участника
виртуальной защищенной сети администрации города Мончегорска

(полное наименование организации, включая организационно-правовую форму)

в лице _____

(должность, фамилия, имя, отчество)

действующего на основании _____

(организационно-распорядительный документ)

просит изготовить дистрибутив ключевой информации на своего уполномоченного представителя – Пользователя виртуальной защищенной сети администрации города Мончегорска, в соответствии с указанными в настоящем заявлении данными:

Наименование юридического лица	<i>Указывается краткое наименование юридического лица Участника</i>
ФИО уполномоченного лица	<i>Указывается Фамилия Имя Отчество уполномоченного лица</i>
Место нахождения (адрес установки абонентского пункта)	<i>Указывается место установки программного обеспечения</i>
Направления связи для организации защищенного обмена информацией	<i>Указывается перечень участников Защищенной сети, которых необходимо включить в направления связи (если требуется)</i>
Перечень информационных ресурсов, к которым необходим доступ	<i>Указывается перечень информационных ресурсов Защищенной сети администрации города, к которым предполагается получить доступ (если требуется)</i>

(*Все поля заполняются максимально полно. Фамилия, имя, отчество впечатываются в **ИМЕНИТЕЛЬНОМ ПАДЕЖЕ**, все поля заполняются исключительно в печатном виде. Заполнение "от руки" **НЕДОПУСТИМО**)

Уполномоченное лицо _____

(Подпись)

(Инициалы/Фамилия)

Ответственный пользователь _____

(Подпись)

(Инициалы/Фамилия)

Руководитель организации _____

(Подпись)

(Инициалы/Фамилия)

М.П.

Настоящим, _____

(фамилия, имя, отчество уполномоченного лица)

соглашается с обработкой своих персональных данных администрацией города Мончегорска и признаёт, что персональные данные, заносимые в дистрибутив ключевой информации, относятся к общедоступным персональным данным. Настоящее согласие может быть отозвано мной путем подачи заявления в письменном виде в адрес администрации города Мончегорска.

Приложение № 3
к Регламенту подключения
к виртуальной защищённой сети
администрации города Мончегорска

ДОВЕРЕННОСТЬ
на получение средств криптографической защиты информации

Дата выдачи

(дата прописью)

(наименование организации)

в лице _____

(должность и ФИО руководителя - полностью)

действующего на основании _____

настоящей доверенностью уполномочивает _____

(должность и ФИО – полностью)

паспорт серии _____ № _____, выдан " ____ " _____ года

(кем выдан)

_____ представлять интересы

(ФИО и должность уполномоченного лица)

_____ и получить

средства криптографической защиты информации (СКЗИ), а также дистрибутивы ключевой информации виртуальной защищенной сети "ViPNet" администрации города Мончегорска и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Ответственным пользователем в _____

(наименование организации)

за эксплуатацию СКЗИ назначен _____

(Ф.И.О., занимаемая должность)

Доверенность действительна до " ____ " _____ 20__ года и дана без права передоверия.

Подпись лица, получившего доверенность _____

(подпись)

Руководитель _____

(Подпись)

(Инициалы/Фамилия)

М.П.

" ____ " _____ 20__ г.

Приложение № 4
к Регламенту подключения
к виртуальной защищённой сети
администрации города Мончегорска

ЗАЯВЛЕНИЕ

на повторное формирование дистрибутива ключевой информации абонентского
пункта виртуальной защищенной сети администрации города Мончегорска

_____ (полное наименование организации, включая организационно-правовую форму)

В лице _____

_____ (должность, фамилия, имя, отчество)

действующего на основании _____

_____ (организационно-распорядительный документ)

просит осуществить повторное формирование и выдачу дистрибутива ключевой
информации абонентского пункта виртуальной защищенной сети администрации города
Мончегорска

_____ (наименование абонентского пункта /идентификатор абонентского пункта)

В СВЯЗИ С _____

_____ причина повторного формирования

Ответственный пользователь _____

_____ (Подпись)

_____ (Инициалы/Фамилия)

Руководитель организации _____

_____ (Подпись)

_____ (Инициалы/Фамилия)

М.П.

Приложение № 5
к Регламенту подключения
к виртуальной защищённой сети
администрации города Мончегорска

УВЕДОМЛЕНИЕ
о компрометации криптографических ключей

Настоящим уведомляю о компрометации криптографических ключей абонентского пункта виртуальной защищенной сети администрации города Мончегорска ViPNet №1105:

(название/идентификатор Абонентского пункта)

сформированных на уполномоченного представителя _____

(ФИО пользователя)

использовавшихся в _____

(наименование Участника (организации))

Компрометация криптографических ключей произошла по причине (подчеркнуть):

- увольнение сотрудников, имевших доступ к ключевой информации;
- доступа к компьютеру пользователя неуполномоченных лиц;
- обнаружения на компьютере пользователя вредоносного кода (вирусов, троянских программ и т.д.);
- иные причины: _____

Данные ключи прошу считать скомпрометированными и выведенными из действия с _____ час. _____ мин. московского времени "___" _____ 20__ г.

Ответственный пользователь _____

(Подпись)

(Инициалы/Фамилия)

Руководитель организации _____

(Подпись)

(Инициалы/Фамилия)

М.П.

"___" _____ 20__ г.

Примечание:

1. Дата и время вывода криптографических ключей из действия, указываемые в настоящем Уведомлении, не могут быть ранее даты и времени получения данного Уведомления Администратором Защищенной сети администрации города или получения сообщения о компрометации Администратором Защищенной сети администрации города по телефону или иным путем.

2. В случае если Ответственный пользователь/Пользователь Участника, формирующий настоящее Уведомление, ранее сообщил Администратору Защищенной сети администрации города о компрометации данных криптографических ключей по телефону, то в настоящем Уведомлении время и дата вывода криптографических ключей из действия определяется временем и датой соответствующего сообщения по телефону.

Приложение № 6
к Регламенту подключения
к виртуальной защищённой сети
администрации города Мончегорска

*(Оформляется на бланке
Организации-заявителя)*

Главе администрации
города Мончегорска

Садчикову В.И.

Об отключении от виртуальной защищённой
сети администрации города Мончегорска

Прошу произвести отключение _____

(наименование Участника (организации))

от виртуальной защищённой сети администрации города Мончегорска ViPNet №1105, а также считать все криптографические ключи абонентских пунктов скомпрометированными и выведенными из действия с ____ час. ____ мин. московского времени "___" _____ 20__ г.

(Должность руководителя)

(Подпись)

(Инициалы/Фамилия)

**ТИПОВОЕ СОГЛАШЕНИЕ № _____
об установлении межсетевого взаимодействия**

г. Мурманск

"__" _____ 20__ г.

Администрация муниципального округа город Мончегорск с подведомственной территорией Мурманской области (сокращенное наименование - Администрация города Мончегорска), в лице главы администрации города _____, действующего на основании Устава города, в дальнейшем именуемое "Администрация", с одной стороны, и

в лице _____, действующего на основании _____, именуемое в дальнейшем "_____", с другой стороны, совместно именуемые "Стороны", заключили настоящее Соглашение о нижеследующем:

1. Предмет соглашения

1.1. Стороны договорились об установлении межсетевого взаимодействия и доверия между сетевыми узлами ViPNet-сети "_____" (далее – ViPNet № _____) и сетевыми узлами ViPNet-сети "_____" (далее – ViPNet № _____). Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между разрешенными сетевыми узлами ViPNet-сетей Сторон.

1.2. Отношения между Сторонами регулируются следующими нормативными документами:

- Федеральным законом от 27.07.2006 №149-ФЗ "Об информации, информационных технологиях и о защите информации";

- Федеральным законом от 06.04.2011 № 63-ФЗ "Об электронной подписи";

- Приказом ФСБ РФ 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".

1.3. Взаимодействие Сторон осуществляется на безвозмездной основе.

2. Права и обязанности сторон

2.1. При организации межсетевого взаимодействия "_____" принимает на себя следующие права и обязанности:

2.1.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet № _____ в границах своей зоны ответственности.

2.1.2. Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet № _____ согласно разделу 3.

2.1.3. Определяет сотрудников, ответственных за взаимодействие в рамках настоящего Соглашения (далее – уполномоченные лица), и сообщает "_____" об

определении таких уполномоченных лиц с указанием их контактных данных (Приложение №5).

2.2. При организации межсетевого взаимодействия "_____" принимает на себя следующие права и обязанности:

2.2.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet №____ в границах своей зоны ответственности.

2.2.2. Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet №____ в соответствии с разделом 3 настоящего соглашения.

2.2.3. Определяет уполномоченных лиц, ответственных за взаимодействие в рамках настоящего Соглашения, и сообщает "_____" об определении таких уполномоченных лиц с указанием их контактных данных.

2.3. Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью (далее – ЦУС) ViPNet-сетей. Экспортируемые данные импортируются в ЦУС соответствующей сети (Приложение №1).

3. Организация межсетевого взаимодействия

3.1. Ответственными лицами Сторон для организации межсетевого взаимодействия являются Администраторы ЦУС. На начальном этапе организуется межсетевое взаимодействие только между абонентскими пунктами (далее – АП) Администраторов ЦУС Сторон через шлюзовые ViPNet-Координаторы в соответствии с технической документацией на программное обеспечение (далее – ПО) ViPNet-Администратор. Этим обеспечивается установление доверия между ViPNet-сетями Сторон.

3.2. По завершении процедуры организации межсетевого взаимодействия между ViPNet №____ и ViPNet №____, подписывается Протокол установления межсетевого взаимодействия (Приложение №2).

3.3. При необходимости установления дополнительных связей между сетевыми узлами Сторон Администраторы ЦУС устанавливают данное взаимодействие руководствуясь технической документацией на ПО ViPNet-Администратор на основании заявки, форма которой указана в (Приложении №3) к настоящему Соглашению. Экземпляр оформленной заявки может быть передан Администратору ЦУС стороной-инициатором в электронном виде на абонентском пункте Администратора.

3.4. После согласования обновленного списка сетевых узлов Администраторы ViPNet-сетей обмениваются соответствующими экспортами и производят соответствующие действия для установления связи между такими узлами.

3.5. Список подключенных сетевых узлов между абонентами ViPNet №____, и ViPNet №____ отображается в Матрице связи (Приложение №4).

3.6. Матрица связи дополняется (изменяется) по мере изменении данных, указанных в списке подключенных сетевых узлов.

4. Проведение профилактических мероприятий

4.1. Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности Стороны осуществляют при соблюдении следующих условий:

– о сроках проведения профилактических мероприятий другая Сторона должна быть оповещена заблаговременно, не позднее, чем за 3 (три) рабочих дня до дня проведения профилактических мероприятий.

4.2. В случае возникновения необходимости проведения технических работ, следствием которых может быть временное прекращение работоспособности программных и программно-аппаратных комплексов "ViPNet", Сторона-инициатор должна уведомить другую Сторону любым удобным способом.

5. Ответственность сторон

5.1. Стороны несут ответственность за обеспечение безопасности информации, передаваемой по средствам программных и программно-аппаратных комплексов "ViPNet" в границах своей зоны ответственности согласно законодательству Российской Федерации.

5.2. Стороны не несут ответственность за содержание информации, передаваемой с применением технологии "ViPNet".

6. Сроки действия соглашения

6.1. Настоящее Соглашение вступает в силу с момента его подписания, и действует бессрочно.

6.2. Настоящее Соглашение может быть расторгнуто по обоюдному согласию Сторон, либо в одностороннем порядке с предупреждением другой Стороны за два месяца до расторжения Соглашения.

7. Форс-мажор

7.1. При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2. Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую Сторону в течение 3 (трех) рабочих дней с предоставлением документов, подтверждающих наличие данных обстоятельств.

7.3. Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

8. Дополнительные условия

8.1. В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

8.2. При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между ViPNet №_____ и ViPNet №_____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

8.3. Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

8.4. В случае изменения наименования, адреса места нахождения или других реквизитов одной из Сторон, Сторона письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

8.5. Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8.6. К настоящему Соглашению прилагаются в качестве неотъемлемой части следующие приложения:

8.6.1. Приложение №1. Состав защищенных сетей и границы зоны ответственности сторон.

8.6.2. Приложение №2. Форма протокола установления межсетевого взаимодействия.

8.6.3. Приложение №3. Заявка на добавление абонентских пунктов в экспорт сети ViPNet №_____.

8.6.4. Приложение №4. Матрица связей между сетевыми узлами.

8.6.5. Приложение №5. Список уполномоченных лиц.

9. Адреса и реквизиты сторон

**Администрация муниципального округа
город Мончегорск с подведомственной
территорией Мурманской области**

Сокращенное наименование:

Администрация города Мончегорска.

ИНН 5107110100

КПП 510701001

ОГРН 1025100654446

Юридический адрес: 184511, Мурманская
область, г. Мончегорск, пр. Metallургов,
д.37

Фактический адрес: 184511, Мурманская
область, г. Мончегорск, пр. Metallургов,
д.37

Тел. (81536) 50000, 50019

Факс: (81536) 72360

E-mail: pochta@monchegorsk-adm.ru

Глава администрации города

Руководитель

_____/_____/_____
М.П.

_____/_____/_____
М.П.

Состав виртуальных защищенных сетей и границы зоны ответственности сторон

1. Состав защищенной сети "_____".
 - 1.1. Состав защищенной сети "_____" включает в себя:
 - ViPNet-Администратор – программный комплекс для настройки и управления защищенной сетью "_____" (ViPNet №_____);
 - Шлюзовой ViPNet-Координатор – сетевой узел, через который проходит весь межсетевой обмен со стороны "_____" (ViPNet №_____).
 - Сетевые узлы – абонентские пункты и координаторы ViPNet №_____.
 2. Состав защищенной сети "_____".
 - 2.1. Состав защищенной сети "_____" включает в себя:
 - ViPNet-Администратор – программный комплекс для настройки и управления защищенной сетью "_____" (ViPNet №_____);
 - Шлюзовой ViPNet-Координатор – сетевой узел, через который проходит весь межсетевой обмен со стороны "_____" (ViPNet №_____).
 - Сетевые узлы – абонентские пункты и координаторы ViPNet №_____.
 3. Границы зоны ответственности Сторон
 - 3.1. ГОБУ "ЦИТ МО" несет ответственность за работоспособность программных и программно-аппаратных комплексов ViPNet №_____.
 - 3.2. "_____" несет ответственность за работоспособность программных и программно-аппаратных комплексов ViPNet №_____.

**Администрация муниципального округа
город Мончегорск с подведомственной
территорией Мурманской области**

Глава администрации города

Руководитель

_____/_____/_____
М.П.

_____/_____/_____
М.П.

ФОРМА ПРОТОКОЛА
установления межсетевого взаимодействия

г. Мурманск

"__" _____ 20__ г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet № _____ и ViPNet № _____.

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО

4. Передача начального и ответного экспорта между сетями ViPNet № _____ и ViPNet № _____ осуществлялась через специалиста, уполномоченного на данные действия.

5. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети ViPNet № _____.

6. Для установления межсетевого взаимодействия были назначены серверы маршрутизаторы для организации шлюза:

- в сети ViPNet № _____ – "_____";
- в сети ViPNet № _____ – "_____".

7. При установлении межсетевого взаимодействия в части создания связей между сетевыми узлами были произведены импорты справочников из сети ViPNet № _____ и сети ViPNet № _____.

8. Стороны обязуются производить изменения в настройках и структуре защищенных сетей, которые могут привести к нарушению межсетевого взаимодействия, только после предварительного согласования.

Администратор ViPNet № _____

Администратор ViPNet № _____

Должность

Должность

_____ / _____ / _____

_____ / _____ / _____

**Форма заявки на добавление абонентских пунктов
в экспорт сети ViPNet № _____
" ____ " _____ 20__ г.**

Просим Вас организовать защищенный канал связи в соответствии со следующей информацией:

1. Полное наименование организации	
2. Юридический адрес организации с индексом	
3. Количество необходимых для регистрации Абонентских пунктов	
4. Наименование Абонентских пунктов (не более 47 символов включая пробелы)	
5. ФИО Абонента зарегистрированного на Абонентском пункте	
6. ФИО Администратора ViPNet-сети	
7. Контактный телефон, e-mail администратора ViPNet-сети	
8. Номер ViPNet-сети	
9. Перечень информационных систем, абонентских пунктов, к которым необходим доступ	

Администратор ViPNet-сети № _____

_____ (фамилия, и.о.)

Матрица связей между сетевыми узлами ViPNet №1105 и ViPNet № _____

ViPNet № 1105 ViPNet № _____				

Администратор ViPNet №1105

Должность

_____ / _____ /

Администратор ViPNet № _____

Должность

_____ / _____ /

Список уполномоченных лиц "Администрации"

№ п/п	Ф. И. О.	Должность	Контактный телефон	Роль	Название АП
1				Администратор защищенной сети	Администратор сети ИОГВ МО
2				Администратор защищенной сети	Администратор сети ИОГВ МО
3				Администратор защищенной сети	Администратор сети ИОГВ МО

Список уполномоченных лиц _____

№ п/п	Ф. И. О.	Должность	Контактный телефон	Роль	Название АП
1					
2					
3					
