УТВЕРЖДАЮ

Директор
ТФОМС Мурманской области

_____ В.А.Акульчев

«___» _____ 2012 г.

ПОЛОЖЕНИЕ
О ЗАЩИЩЁННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET ТЕРРИТОРИАЛЬНОГО ФОНДА ОБЯЗАТЕЛЬНОГО МЕДИЦИНСКОГО СТРАХОВАНИЯ МУРМАНСКОЙ ОБЛАСТИ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

ViPNet [Администратор]	-	программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet.
ViPNet [Клиент]	-	программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы.
ViPNet [Координатор]	-	программное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet.
VPN (Virtual Private Network)	-	обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.
Абонент Защищённой сети	-	назначенный приказом руководителя, сотрудник Участника системы здравоохранения, использующий для выполнения своих служебных обязанностей сервисы и информационные системы Защищённой сети.
Абонентский пункт	-	персональный компьютер с установленным программным обеспечением ViPNet [Клиент].
Автопроцессинг	-	автоматическая обработка файлов и писем в программе «Деловая почта», в соответствии с различными правилами задаваемыми пользователем.
Владелец информационных систем	-	участник, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством.
Владелец сертификата ключа проверки электронной подписи	-	физическое лицо, на имя которого Удостоверяющим центром выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим ключом электронной подписи, позволяющим с помощью средств электронной подписи создавать свою электронную подпись в электронных документах (подписывать электронные документы).
Главный администратор Защищённой сети	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области осуществляющий общую политику администрирования всей Защищённой сети.
Информационная система	-	совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Ключ проверки электронной подписи	-	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее - проверка электронной подписи).
Ключ электронной подписи	-	уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи.
Ключевой носитель	-	носитель, содержащий один или несколько ключей.
Компрометация ключа	-	утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.
Координатор Защищённой сети	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области, определяющий общую стратегию развития Защищённой сети.
Корпоративная информационная система МТФОМС	-	информационная система, участниками электронного взаимодействия в которой являются Участники системы здравоохранения.
Локальный администратор Защищённой сети	-	назначенный приказом сотрудник Участника системы здравоохранения, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному участнику.
Несанкционированный доступ	-	доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах путём изменения (повышения, фальсификации) своих прав доступа.
Пользователь Удостоверяющего центра	-	физическое лицо (уполномоченный представитель Участника, присоединившегося к Регламенту Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области), зарегистрированное в Удостоверяющем центре.

Сертификат ключа проверки электронной подписи	-	электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Список отозванных сертификатов	-	документ на бумажном носителе или электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения их срока действия.
Средство электронной подписи	-	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. В Защищённой сети, данные функции реализованы в модуле «Деловая почта».
Технология ViPNet	-	технология, предназначенная для построения виртуальных защищённых сетей, путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами на базе средства криптографической защиты информации «Домен-К».
Удостоверяющий центр	-	Территориальный фонд обязательного медицинского страхования Мурманской области, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные законодательством.
Уполномоченное лицо Удостоверяющего центра	-	назначенный приказом директора сотрудник Территориального фонда обязательного медицинского страхования Мурманской области, наделённый полномочиями по заверению сертификатов ключей проверки электронных подписей и списков отозванных сертификатов.
Усиленная неквалифицированная электронная подпись (далее – неквалифицированная ЭП)	-	ЭП, полученная, в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяющая определить лицо, подписавшее электронный документ и обнаружить факт внесения изменений в электронный документ после момента его подписания.

Участник системы здравоохранения	-	обладатель информации, формирующейся в области здравоохранения, осуществляющий деятельность, направленную на реализацию прав граждан на охрану здоровья и медицинскую помощь.
Центр управления сетью	-	аппаратные или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети.
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.
Электронный документ	-	документ, в котором информация представлена в электронно-цифровой форме, и который может быть представлен в виде файла, хранящегося на носителе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Положение о защищённой виртуальной сети VipPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Положение) разработано в соответствии с:

- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской федерации»;
- Федеральным законом от 10 января 2002 года № 1-ФЗ «Об электронной цифровой подписи»;
- Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Данное Положение определяет состав и устройство защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Защищённая сеть), устанавливает принципы подключения и использования сервисов Защищённой сети, а также правила информационной безопасности, функции и полномочия участников Защищённой сети.

3. НАЗНАЧЕНИЕ ЗАЩИЩЁННОЙ СЕТИ

Основными задачами, которые решает Защищённая сеть, являются:

3.1. Организация защищённого информационного взаимодействия между Участниками системы здравоохранения (далее – Участники).

3.2. Уменьшение вероятности потери, искажения и хищения информации при её передачи между Участниками.

3.3. Организация защищённого доступа к информационным ресурсам Участников, в целях реализации Федерального закона от 29 ноября 2010 года №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и Основ законодательства Российской Федерации об охране здоровья граждан №5487-1 от 22 июля 1993 года.

4. СТРУКТУРА И СОСТАВ ЗАЩИЩЁННОЙ СЕТИ

4.1. Защищённая сеть представляет собой территориально распределённую информационно-телекоммуникационную сеть, объединяющую абонентские пункты Участников по технологии ViPNet.

4.2. Центр управления Защищённой сетью расположен в Территориальном фонде обязательного медицинского страхования Мурманской области (далее –ТФОМС Мурманской области).

4.3. Связь абонентских пунктов Участников осуществляется по каналам связи, которые используются Участниками.

4.4. Программное обеспечение, обеспечивающее функционирование Защищённой сети:

ViPNet [Администратор]

ViPNet [Координатор]

ViPNet [Клиент]

4.5. Основными активными компонентами Защищённой сети являются серверы и абонентские пункты.

4.6. В составе Защищённой сети функционируют следующие основные виды серверов: файловые серверы, серверы ViPNet [Координатор], серверы баз данных, расположенные в специально оборудованных помещениях с ограниченным доступом.

4.6.1. Файловые серверы.

Выделенный сервер, оптимизированный для выполнения файловых операций ввода-вывода, предназначен для хранения файлов Участников.

4.6.2. Серверы ViPNet [Координатор].

Многофункциональные серверы, осуществляющие, в зависимости от настроек, следующие основные функции:

-маршрутизацию почтовых и управляющих защищённых сообщений;

-регистрацию и предоставление информации о состоянии объектов Защищённой сети;

-фильтрацию трафика от источников, не входящих в состав Защищённой сети, в соответствии с заданной политикой безопасности.

Функциональность ViPNet [Координатора] определяется Центром управления Защищённой сетью и формируемыми им справочниками и маршрутными таблицами.

4.6.3. Серверы баз данных.

Серверы, предназначенные для обслуживания баз данных, отвечающие за целостность и сохранность данных, а также обеспечивающие операции ввода-вывода информации при доступе Участников Защищённой сети к информационным системам.

4.6.4. Абонентский пункт.

IBM совместимый компьютер соответствующий следующим требованиям:

-процессор не менее Pentium III;

-оперативная память не менее 512 Мбайт;

-операционная система Windows 2000 (32 бит) SP4, Windows XP (32 бит), Windows Server 2003 (32 бит), Windows Vista (32/64 бит), Windows Server 2008 (32/64 бит), Windows 7 (32/64 бит), Windows Server 2008 R2 ;

-установленное программное обеспечение ViPNet [Клиент];

-наличие сетевого интерфейса, обеспечивающего соединение с сервером ViPNet [Координатор].

4.7. Удостоверяющий центр корпоративного уровня Защищённой сети.

Компонент ПО ViPNet [Администратор], служащий для организации обмена юридически значимыми электронными документами в рамках Защищённой сети с применением электронной цифровой подписи.

4.7.1. Функции, порядок и условия предоставления Удостоверяющим центром корпоративного уровня Защищённой сети возможности участвовать в обмене юридически значимыми электронными документами с применением электронной цифровой подписи

определены в Регламенте Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее - Регламент УЦ).

4.8. Режим работы Защищённой сети.

4.8.1. Файловые серверы, серверы баз данных, серверы ViPNet [Координатор] работают круглосуточно, 7 дней в неделю, за исключением перерывов для проведения аварийно-ремонтных и планово-профилактических работ.

4.8.2. Удостоверяющий центр корпоративного уровня Защищенной сети в части приёма заявлений в бумажной форме и изготовления сертификатов ключей проверки электронной подписи осуществляет работу с 8.30-13.00 и с 14.00-17.30 в будние дни. Выходными днями являются: суббота, воскресенье, а также дни общенациональных праздников.

5. КАТЕГОРИИ ПОЛЬЗОВАТЕЛЕЙ ЗАЩИЩЁННОЙ СЕТИ

5.1. Координатор Защищённой сети.

5.1.1. Пользователь данной категории определяет общую стратегию развития Защищённой сети, разрабатывает регламентирующие документы для участников, контролирует и анализирует процесс развития Защищённой сети.

5.1.2. Координатором Защищённой сети (далее – Координатор) является сотрудник ТФОМС Мурманской области, назначенный приказом директора ТФОМС Мурманской области.

5.1.3. Функции и полномочия Координатора определяются в разделе 7 настоящего положения.

5.2. Главный администратор Защищённой сети.

5.2.1. Пользователь данной категории определяет и осуществляет общую политику администрирования всей Защищённой сети.

5.2.2. Главным администратором Защищённой сети (далее - Главный администратор) является сотрудник ТФОМС Мурманской области, назначенный приказом директора ТФОМС Мурманской области.

5.2.3. Функции и полномочия Главного администратора определяются в разделе 8 настоящего Положения.

5.3. Локальный администратор Защищённой сети.

5.3.1. Пользователь данной категории осуществляет администрирование информационных систем и абонентских пунктов, принадлежащих Участнику.

5.3.2. Локальным администратором Защищённой сети (далее – Локальным администратором) является сотрудник Участника, назначенный приказом соответствующего Участника.

5.3.3. Функции и полномочия Локального администратора определяются в разделе 9 настоящего Положения.

5.4. Абонент Защищённой сети.

5.4.1. Пользователь данной категории использует для выполнения своих служебных обязанностей сервисы, ресурсы и информационные системы Защищённой сети.

5.4.2. Абонентом Защищённой сети (далее – Абонентом) является сотрудник Участника, назначенный приказом соответствующего Участника.

5.4.3 Полномочия Абонента определяются его служебными обязанностями.

5.5 Уполномоченное лицо Удостоверяющего центра

5.5.1. Пользователь данной категории осуществляет сертификацию открытых ключей подписи для пользователей, вывод ключей подписи из действия, заверение ключей подписей и списков отозванных сертификатов.

5.5.2. Уполномоченное лицо Удостоверяющего центра (далее – Уполномоченное лицо) является сотрудник ТФОМС Мурманской области, назначенный приказом директора ТФОМС Мурманской области.

5.5.3. Функции и полномочия Уполномоченного лица определяются в разделе 10 настоящего Положения.

5.6 Пользователь Удостоверяющего центра .

5.6.1. Пользователь данной категории осуществляет обмен электронными документами и заверяет их своей электронной цифровой подписью.

5.6.2. Пользователем Удостоверяющего центра (далее – Пользователем УЦ) является физическое лицо (уполномоченный представитель Участника), зарегистрированное в Удостоверяющем центре в соответствии с Регламентом УЦ.

5.6.3. Права и обязанности Пользователей УЦ определены в разделе 11 настоящего Положения.

6. СЕРВИСЫ ЗАЩИЩЁННОЙ СЕТИ

6.1. Абоненты получают доступ к следующим сервисным службам:

-защищённая электронная почта;

-защищённый файловый обмен;

-оперативный обмен защищёнными сообщениями;

-доступ к ресурсам и информационным системам Защищённой сети.

6.2. Защищённая электронная почта.

Сервис, реализованный на базе модуля «Деловая почта» входящего в состав программного обеспечения ViPNet [Клиент], выполняющий функции почтового клиента защищённой почтовой службы, функционирующей в рамках Защищённой сети.

6.2.1. Основными функциями модуля «Деловая почта» являются:

-передача электронных сообщений, а также прикреплённых к ним файлов по открытым каналам связи с защитой на всём маршруте следования от отправителя до получателя;

-организация по установленным правилам защищённого автопроцессинга стандартных документов;

-подтверждение личности отправителя, с помощью электронной подписи Пользователя УЦ, полученной в соответствии с Регламентом УЦ;

-подтверждение получения и использования сообщений, а также даты, времени получения и личности получателей.

6.3. Защищённый файловый обмен.

Сервис, позволяющий Абонентам обмениваться любыми файлами без установки дополнительного программного обеспечения или использования функций операционной системы.

6.3.1. Основными функциями защищённого файлового обмена являются:

-обмен файлами между абонентами через защищённую транспортную сеть ViPNet;

-гарантированная доставка и возобновление передачи файлов при обрыве связи.

6.4. Оперативный обмен защищёнными сообщениями.

Сервис, предназначенный для обмена сообщениями в режиме реального времени между абонентами Защищённой сети.

6.4.1. Основными функциями оперативного обмена, защищёнными сообщениями являются:

-передача сообщений между абонентами в защищённом виде исключающим постороннее вмешательство;

-обмен сообщениями в режиме конференции;

-сохранение результатов в протокол.

6.5. Защищённый доступ к информационным системам.

Сервис, обеспечивающий возможность защищённой работы в режиме «клиент-сервер» с установленным программным обеспечением ViPNet [Клиент] на серверах и рабочих станциях.

6.5.1. Основными функциями защищённого доступа к информационным системам являются:

-защита трафика при обращении к серверам баз данных;

-разграничение доступа к информационным системам.

7. ФУНКЦИИ И ПОЛНОМОЧИЯ КООРДИНАТОРА

7.1. Обязанности Координатора:

-разработка единых правил формирования, развития и функционирования Защищённой сети;

-разработка регламентирующих документов использования информационных систем, доступ к которым предоставляется с использованием Защищённой сети (совместно с владельцами информационных систем);

-еженедельное формирование в электронном виде реестра Участников и информационных систем, подключенных к Защищённой сети (далее – Реестр);

-еженедельная рассылка Реестра Абонентам, средствами модуля «Деловая почта»;

-разработка предложений по формированию и внедрению компонентов Защищённой сети (совместно с Главным администратором);

-контроль за соблюдением всеми категориями пользователей правил работы и использования компонентов Защищённой сети;

7.2. Права Координатора.

Для выполнения своих обязанностей Координатор имеет право:

-информировать руководителей Участников при невыполнении их сотрудниками требований безопасности и несоблюдения других требований по обеспечению бесперебойного функционирования Защищённой сети;

-запрашивать у Главного администратора информацию о компонентах Защищённой сети;

-принимать решение об отключении или ограничении доступа к информационным системам Защищённой сети в случаях нарушения сотрудниками Участника требований настоящего Положения и Регламента Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области (далее – Регламент).

7.3. Ответственность Координатора.

Координатор несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-неправомерное использование информации циркулирующей в Защищённой сети, к которой Координатор получает доступ в связи с выполнением своих функций.

8. ФУНКЦИИ И ПОЛНОМОЧИЯ ГЛАВНОГО АДМИНИСТРАТОРА

8.1. Главный администратор осуществляет оперативно-административное руководство Защищённой сетью. Главный администратор несёт персональную ответственность за бесперебойное функционирование Защищённой сети, в рамках своей компетенции даёт другим пользователям рекомендации, связанные с обеспечением работоспособности Защищённой сети.

8.2. Обязанности Главного администратора:

-поддержка работоспособности и управление режимами работы компьютерного и коммутационного оборудования в Центре управления Защищённой сети;

-проведение мероприятий по модернизации и развитию Защищённой сети (совместно с Координатором);

-предоставление Участникам, по заявкам их руководителей, доступа к информационным системам Защищённой сети (совместно с Координатором);

-своевременное реагирование на поступившие заявки о неисправностях в работе компонентов Защищённой сети и принятие необходимых мер по их устранению;

-периодические проверки состояния Защищённой сети и своевременное реагирование на попытки несанкционированного доступа;

-предоставление Координатору информации о компонентах Защищённой сети;

-информирование Локальных администраторов о порядке работы и ответственности за нарушение настоящего Положения и Регламента;

-информирование Локальных администраторов о проводимых работах по обслуживанию и возможных перебоях в работе Защищённой сети;

8.3. Права Главного администратора.

Для выполнения своих обязанностей Главный администратор имеет право:

-информировать руководителей Участников при невыполнении их сотрудниками требований безопасности и несоблюдении других требований по обеспечению бесперебойного функционирования Защищённой сети (по согласованию с Координатором);

-вносить предложения по привлечению для технического обслуживания и администрирования оборудования Защищённой сети сторонние организации, с учётом требований действующего законодательства;

-производить отключение или ограничение доступа к информационным системам Защищённой сети в случаях нарушения сотрудниками Участника требований настоящего Положения и Регламента.

8.4. Ответственность Главного администратора.

Главный администратор несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-несвоевременное выявление попыток несанкционированного доступа, приведших к нарушению требований по безопасности Защищённой сети и сбою её функционирования;

-несвоевременное устранение неисправностей в работе компонентов Защищённой сети.

-неправомерное использование информации циркулирующей в Защищённой сети, к которой Главный администратор получает доступ в связи с выполнением своих функций.

9. ФУНКЦИИ И ПОЛНОМОЧИЯ ЛОКАЛЬНОГО АДМИНИСТРАТОРА

9.1. Локальный администратор осуществляет администрирование информационных систем и абонентских пунктов принадлежащих Участнику. Локальный администратор несёт персональную ответственность за бесперебойное функционирование принадлежащих Участнику информационных систем и абонентских пунктов, в рамках своей компетенции даёт другим пользователям рекомендации, связанные с обеспечением работоспособности Защищённой сети.

9.2. Обязанности Локального администратора:

-подключение Абонентских пунктов и информационных систем к Защищённой сети;

-формирование учётных записей для организации доступа к информационным системам;

-информирование Абонентов Защищённой сети о порядке работы в Защищённой сети и ответственности за нарушение данного Положения;

-принятие мер по пресечению несанкционированного доступа к компонентам Защищённой сети со стороны Абонентов;

-уведомление руководителя Участника и Главного администратора о случаях нарушений и принятых мерах;

-ознакомление Абонентов с правилами работы и требованиями безопасности Защищённой сети.

9.3. Права Локального администратора.

Для выполнения своих обязанностей Локальный администратор имеет право:

-сообщать непосредственному руководителю, Главному администратору и Координатору о действиях Абонентов, осуществивший несанкционированный доступ к ресурсам Защищённой сети или нарушившим другие требования по обеспечению безопасности информации и бесперебойной работы Защищённой сети;

-обращаться к Главному администратору для решения вопросов по предоставлению доступа к информационным системам Участников, после получения согласия владельца соответствующей информационной системы;

-предоставлять Координатору предложения, касающиеся разработки единых правил формирования, развития и работы Защищённой сети.

9.4. Ответственность Локального администратора.

Локальный администратор несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-несвоевременное выявление попыток несанкционированного доступа, приведших к нарушению требований по безопасности Защищённой сети и сбою её функционирования;

-несвоевременное устранение неисправностей в работе компонентов Защищённой сети.

-неправомерное использование информации, циркулирующей в Защищённой сети, к которой Локальный администратор получает доступ в связи с выполнением своих функций.

10. ФУНКЦИИ И ПОЛНОМОЧИЯ УПОЛНОМОЧЕННОГО ЛИЦА УДОСТОВЕРЯЮЩЕГО ЦЕНТРА

10.1. Уполномоченное лицо осуществляет регистрацию Пользователей УЦ в соответствии с Регламентом Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области, сертификация ключей проверки электронной подписи для Пользователей УЦ, вывод ключей подписи из действия, заверение ключей подписей и списков отозванных сертификатов.

10.2. Обязанности Уполномоченного лица:

-внесение в реестр Удостоверяющего центра регистрационной информации о Пользователях УЦ;

-формирование и обновление справочно-ключевой информации для организации защищённого обмена в рамках Защищённой сети;

-изготовление сертификатов ключей проверки электронной подписи Пользователей УЦ в электронной форме;

-формирование ключей электронной подписи и ключей проверки электронной подписи , с записью их на ключевой носитель;

-ведение реестра изготовленных сертификатов ключей проверки электронной подписи Пользователей УЦ;

-аннулирование (отзыв) сертификатов ключей проверки электронной подписи по обращениям Владельцев сертификатов открытых ключей;

-приостановление и возобновление действия сертификатов ключей проверки электронной подписи по обращению Владельцев сертификатов открытых ключей;

-подтверждение подлинности электронных подписей в документах представленных в электронной форме, по обращениям Пользователей УЦ;

-обеспечение безопасности электронного ключа подписи Уполномоченного лица;

10.3. Права Уполномоченного лица:

В процессе выполнения своих обязанностей Уполномоченное лицо имеет право:

-отказать в регистрации пользователям, в случае нарушения порядка регистрации определённым Регламентом Удостоверяющего центра корпоративного уровня Защищённой виртуальной сети ViPNet Территориального фонда обязательного медицинского страхования Мурманской области;

-аннулировать (отозвать) сертификат ключа проверки электронной подписи Пользователя УЦ в случае установления факта компрометации соответствующего ключа электронной подписи, с уведомлением Владельца аннулированного (отозванного) сертификата ключа проверки электронной подписи и указанием причин;

-в одностороннем порядке приостановить действие сертификата ключа проверки электронной подписи Пользователя УЦ, с обязательным уведомлением Владельца приостановленного сертификата ключа проверки электронной подписи и указанием обоснованных причин.

10.4. Ответственность Уполномоченного лица.

Уполномоченное лицо несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-неправомерное использование информации циркулирующей в Защищённой сети, к которой Уполномоченное лицо получает доступ в связи с выполнением своих функций.

11. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ УЦ

11.1. Права Пользователя УЦ.

Пользователи УЦ имеет право:

-обратиться в Удостоверяющий центр для изготовления сертификата ключа проверки электронной подписи;

-обратиться в Удостоверяющий центр для внесения в реестр Удостоверяющего центра регистрационной информации о Пользователе УЦ, с целью в дальнейшем стать Владельцем сертификата ключа проверки электронной подписи;

-получить список аннулированных (отозванных) и приостановленных сертификатов ключей проверки электронной подписи, изготовленный Удостоверяющим центром;

-применять сертификаты ключа проверки электронной подписи в электронной форме для проверки электронной подписи электронного документа в соответствии со сведениями, указанными в сертификате ключа проверки электронной подписи;

-применять список аннулированных (отозванных) и приостановленных сертификатов ключей проверки электронной подписи, изготовленных Удостоверяющим центром, для проверки статуса сертификатов ключей проверки электронной подписи;

-обратиться в Удостоверяющий центр для аннулирования (отзыва) сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи;

-обратиться в Удостоверяющий центр для приостановления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи;

-обратиться в Удостоверяющий центр для возобновления действия сертификата ключа проверки электронной подписи в течение срока действия соответствующего ключа электронной подписи;

11.2. Обязанности Пользователя УЦ:

-лица, проходящие процедуру регистрации в реестре Удостоверяющего центра, обязаны предоставить регистрационную и идентифицирующую информацию в объёме, определённом положениями Регламента УЦ;

-хранить в тайне ключ электронной подписи, принимая все возможные меры для предотвращения его потери, раскрытия, модифицирования или несанкционированного использования;

-не использовать для электронной цифровой подписи ключ электронной подписи, если известно, что эти ключи используются или использовались ранее другими лицами;

-использовать ключ электронной подписи только для целей, разрешённых соответствующими областями использования, определёнными в сертификате согласно Регламенту УЦ;

-немедленно обратиться в Удостоверяющий центр с заявлением на приостановление действия сертификата ключа проверки электронной подписи в случае потери, раскрытия, искажения личного ключа электронной подписи, а так же в случае если Пользователю УЦ стало известно, что этот ключ используется или использовался ранее другими лицами;

-не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на аннулирование (отзыв) которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на аннулирование (отзыв) сертификата в Удостоверяющий центр по момент времени официального уведомления об аннулировании (отзыве), либо от отказе в аннулировании (отзыве);

-не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, заявление на приостановление действия которого подано в Удостоверяющий центр, в течение времени, исчисляемого с момента времени подачи заявления на приостановление действия сертификата в Удостоверяющий центр по момент времени официального уведомления о приостановлении действия , либо от отказе в приостановлении действия;

-не использовать личный ключ электронной подписи, связанный с сертификатом ключа проверки электронной подписи, который аннулирован (отозван) или действие его приостановлено;

-перед тем как использовать сертификат ключа проверки электронной подписи, изготовленный Удостоверяющим центром, Владелец сертификата должен удостоверится, что назначение сертификата, определённое соответствующими областями использования, определёнными в сертификате согласно Регламенту УЦ, соответствует предполагаемому использованию.

11.3. Ответственность Пользователя УЦ.

Пользователь УЦ несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-неправомерное использование информации, циркулирующей в Защищённой сети, к которой Абонент получает доступ в связи с выполнением своих функций.

12. ОБЩИЕ ПРАВИЛА РАБОТЫ АБОНЕНТОВ

12.1. Абоненты должны быть ознакомлены с правилами работы в Защищённой сети, предусмотренными настоящим Положением и предупреждены о возможной ответственности за их нарушение.

12.2. Абонент обязан:

-знать правила безопасности в Защищённой сети;

-при работе в Защищённой сети выполнять только служебные задания;

-при сообщении тестовых программ о появлении «вирусов» или обнаружении подозрительных действий немедленно доложить своему Локальному администратору;

-предоставлять свой абонентский пункт Локальному администратору для контроля и осуществления административных действий;

-обеспечить безопасность хранения ключевой информации и пароля.

12.3. Абоненту запрещается:

-оставлять не заблокированным и без контроля свой абонентский пункт;

-допускать к подключённому в Защищённую сеть абонентскому пункту посторонних лиц;

-самостоятельно проводить изменения в настройках абонентского пункта;

-передавать пароли и ключевую информацию третьим лицам.

12.4. Абонент имеет право:

-пользоваться информационными системами и сервисами Защищённой сети в рамках предоставленных ему полномочий;

-обращаться к непосредственному руководителю и своему Локальному администратору для решения вопросов использования информационных систем Участников.

12.5. Ответственность Абонента.

Абонент несёт ответственность за:

-невыполнение требований настоящего Положения, Регламента и Регламента УЦ, а также других актов, регулирующих работу Защищённой сети;

-неправомерное использование информации, циркулирующей в Защищённой сети, к которой Абонент получает доступ в связи с выполнением своих функций.

12.6. Ответственность за допуск Абонента к работе в Защищённой сети и предоставленные ему полномочия, несёт руководитель Участника, назначивший Абонента в соответствии с Регламентом.

13. ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ

13.1. Технические мероприятия по обслуживанию компонентов Защищенной сети и информационных систем проводятся Главным администратором, при необходимости с привлечением Локального администратора соответствующего Участника.

13.2. В случае возникновения производственной необходимости проведения аварийных и планово-профилактических работ, Защищённая сеть может быть закрыта для доступа.

13.3. Плановые работы проводятся по графику разрабатываемому Главным администратором.

13.4. К плановым работам относятся:

-реконфигурирование Защищённой сети;

-установка операционных систем;

-техническое обслуживание компонентов Защищённой сети;

-другие виды работ, необходимость которых определяется Главным администратором по согласованию с Координатором.

13.5. О проведение плановых работ Главный администратор уведомляет Локальных администраторов Участников Защищённой сети не менее чем за 24 часа, до намеченного срока начала работ.

13.6. Функционирование Защищенной сети в аварийном режиме.

-для защиты компонентов Защищённой сети от сбоев электропитания файловые серверы, серверы ViPNet [Координатор], серверы баз данных и абонентские пункты оборудуются источниками бесперебойного питания, мощность которых в случае отключения электропитания обеспечивает возможность корректного завершения выполняемых задач;

-в случае возможных нештатных ситуаций Локальные администраторы, при необходимости с привлечением Главного администратора, восстанавливают работоспособность компонентов Защищённой сети в технологически возможный короткий срок.

14. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ДАННОГО ПОЛОЖЕНИЯ

В случае нарушения требований данного Положения, послуживших причиной сбоя функционирования Защищенной сети или несанкционированного доступа к информации циркулирующей в Защищённой сети, все категории пользователей несут ответственность в соответствии с действующим законодательством.

15. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В НАСТОЯЩЕЕ ПОЛОЖЕНИЕ.

Все изменения и дополнения в настоящее Положение вносятся соответствующим приказом ТФОМС Мурманской области и доводятся до сведения всех Участников по Защищённой электронной почте в течение 1 рабочего дня со дня издания указанного приказа.

ТФОМС Мурманской области не несёт ответственность за несвоевременное получение изменений и дополнений в настоящее Положение вследствие несвоевременного контроля Участником электронных сообщений Защищённой электронной почты.