Министерство здравоохранения
Республика Карелия

ПРИКАЗ

г. Петрозаводск

от «26» января 2022 года № 120

Об утверждении Регламента работы в государственной информационной системе в сфере здравоохранения Республики Карелия «Медицинские информационные системы»

В соответствии с пунктом 8 Положения, утвержденного постановлением Правительства Республики Карелия от 22 ноября 2021 года №527-П «О государственной информационной системе в сфере здравоохранения Республики Карелия «Медицинские информационные системы»,

п р и к а з ы в а ю:

1. Утвердить прилагаемый Регламент работы в государственной информационной системе в сфере здравоохранения Республики Карелия «Медицинские информационные системы».

2. Контроль за исполнением настоящего приказа оставляю за собой.

Министр М.Е. Охлопков

УТВЕРЖДАЮ
Приказом Министерства
здравоохранения Республики Карелия
№ 120 от 26 января 2022 года

Регламент

работы в государственной информационной системе в сфере здравоохранения Республики Карелия

«Медицинские информационные системы»

г. Петрозаводск

2022 г.

ОГЛАВЛЕНИЕ

ПЕРЕЧЕНЬ ИСПОЛЬЗУЕМЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

АИС – автоматизированная информационная система

ИС – информационная система

АПМДЗ – аппаратно-программный модуль доверенной загрузки

АРМ – автоматизированное рабочее место

ГИС – государственная информационная система

ГИСЗ «МИС» - Государственная информационная система в сфере здравоохранения Республики Карелия «Медицинские информационные системы»

ГБУЗ «РМИАЦ» – Государственное бюджетное учреждение здравоохранения Республики Карелия «Республиканский медицинский информационно–аналитический центр»

Обладатель информации, содержащейся в ГИСЗ «МИС» - Министерство здравоохранения Республики Карелия

Оператор ГИСЗ «МИС» – ГБУЗ «РМИАЦ»

Администраторы ГИСЗ «МИС» – сотрудники оператора ГИСЗ «МИС», обеспечивающие ее функционирование

Поставщики информации в ГИСЗ «МИС», Поставщики информации – Министерство здравоохранения Республики Карелия, медицинские организации на территории Республики Карелия с действующей лицензией на осуществление медицинской деятельности, страховые медицинские организации, осуществляющие деятельность в системе обязательного медицинского страхования Республики Карелия, фармацевтические организации, осуществляющие деятельность в системе льготного лекарственного обеспечения Республики Карелия, государственное учреждение «Территориальный фонд обязательного медицинского страхования Республики Карелия».

ИС Поставщика информации – ИС, принадлежащая Поставщику информации по праву собственности или на любом другом основании (исключая компоненты ГИСЗ «МИС»)

Внешний объект - сегмент сети, АРМ, подключаемые (имеющие подключения) к ГИСЗ «МИС», а также ИС Поставщиков информации, подключаемых к ГИСЗ «МИС» с помощью модулей (систем) интеграции

ЗПС – замкнутая программная среда, механизм которой позволяет определить для любого пользователя компьютера перечень программного обеспечения, разрешенного для использования

Инцидент (информационной безопасности), инцидент ИБ - непредвиденное или нежелательное событие (группа событий) безопасности, которое (которые) привело (привели) к негативным последствиям для актива организации

Компьютерный инцидент - факт нарушения и (или) прекращения функционирования информационного ресурса и (или) нарушения безопасности, обрабатываемой таким информационным ресурсом информации, в том числе произошедший в результате компьютерной атаки

Компрометация учетной записи в информационном ресурсе (как тип компьютерного инцидента) - факт проведения компьютерной атаки, в ходе которой нарушитель (злоумышленник) получил идентификационные и/или аутентификационные данные пользователя информационного ресурса

ЗСПД – защищённая сеть передачи данных

ИСПДн – информационная система персональных данных

МЭ – межсетевой экран

МО – медицинская организация

ПАК – программно-аппаратный комплекс

РД – Руководящий документ

Репозиторий (репозиторий программных пакетов) - замкнутая совокупность программных пакетов и метаинформации о них. Репозиторий называется замкнутым, если для каждого бинарного пакета можно вычислить его замыкание, т.е. можно установить пакет в систему с соблюдением всех его зависимостей (ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.)

СДЗ – средство доверенной загрузки

СЗИ – средство защиты информации

СКЗИ – средство криптографической защиты информации

СОВ – средство обнаружения вторжений

ТУ – Технические условия

ФСБ России – Федеральная служба безопасности Российской Федерации.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю

ЭД – эксплуатационная документация

ВВЕДЕНИЕ

Государственная информационная система в сфере здравоохранения Республики Карелия «Медицинские информационные системы» (ГИСЗ «МИС») осуществляет информационное и процессное взаимодействие со следующими информационными системами:

– Единой государственной информационной системой в сфере здравоохранения;

– автоматизированной информационной системой государственного учреждения «Территориальный фонд обязательного медицинского страхования Республики Карелия»;

– информационными системами медицинских организаций Республики Карелия;

– иными информационными системами в случаях, предусмотренных законодательством Российской Федерации.

В состав ГИСЗ «МИС» входят следующие информационные системы:

– информационная система «ПроМед»;

– информационная система «Портал самозаписи на прием к врачу»;

– информационная система «Центры здоровья»;

– информационная система «ТМ:ЦОД».

Функционирование ГИСЗ «МИС» осуществляется на базе телекоммуникационной сети (в том числе защищенной сети передачи данных с использованием средств криптографической защиты информации VipNet) Оператора ГИСЗ «МИС» - ГБУЗ «РМИАЦ».

ГИСЗ «МИС» обеспечивает выполнение следующих функций:

1) поддержка принятия управленческих решений по вопросам развития здравоохранения в Республике Карелия;

2) управление потоками пациентов (электронная регистратура);

3) управление скорой, в том числе скорой специализированной, медицинской помощью (включая санитарно-авиационную эвакуацию);

4) ведение интегрированной электронной медицинской карты;

5) учет сведений о показателях системы здравоохранения, в том числе медико-демографических показателей здоровья населения;

6) ведение специализированных регистров пациентов по отдельным нозологиям и категориям граждан;

7) сбор, хранение и обработка информации об обеспеченности отдельных категорий граждан, в том числе граждан, имеющих право на получение государственной социальной помощи, лекарственными препаратами, специализированными продуктами лечебного питания, медицинскими изделиями;

8) обеспечение оказания медицинской помощи с применением телемедицинских технологий;

9) организация профилактики заболеваний, включая проведение диспансеризации, профилактических медицинских осмотров;

10) ведение учета иммунопрофилактики инфекционных заболеваний;

11) ведение централизованной системы (подсистемы) управления лабораторными исследованиями;

12) ведение централизованной системы (подсистемы) хранения и обработки результатов диагностических исследований (медицинских изображений);

13) обеспечение автоматизации процессов оказания медицинской помощи по отдельным нозологиям и категориям граждан;

14) учет обращения медицинской документации, организация электронного документооборота в сфере охраны здоровья;

15) ведение нормативно-справочной информации в сфере здравоохранения Республики Карелия;

16) централизованное предоставление населению государственных услуг в сфере здравоохранения.

Настоящий Регламент устанавливает порядок и условия доступа к ГИСЗ «МИС».

Требования настоящего Регламента определяют состав, содержание, порядок выполнения работ по подключению к ГИСЗ «МИС» и распространяются на сегменты сети и АРМ, подключаемые (имеющие подключения) к ГИСЗ «МИС», а также на ИС Поставщиков информации, подключаемых к ГИСЗ «МИС» с помощью модулей (систем) интеграции (далее - Внешний объект ГИСЗ «МИС»).

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

1.1. Общее описание и участники информационного взаимодействия.

Обмен информацией в ГИСЗ «МИС» осуществляется в электронном виде, в приоритетном порядке с использованием выделенных сетей связи (VLAN/IPVPN) и сетей связи общего пользования (сети Интернет).

Участники информационного взаимодействия являются: Обладатель информации, содержащейся в ГИСЗ «МИС» ,Оператор ГИСЗ «МИС», Поставщики информации в ГИСЗ «МИС»

Для ГИСЗ «МИС» определён 2 класс защищённости в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 года № 17.

Для персональных данных в ГИСЗ «МИС» определен второй уровень защищенности персональных данных в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119.

На основании Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» ГИСЗ «МИС» является значимым объектом критической информационной инфраструктуры Российской Федерации.

В ГИСЗ «МИС» для защиты информации конфиденциального характера используются сертифицированные шифровальные (криптографические) средства на базе продуктов семейства ViPNet (сеть № 934). Для организации защищенного взаимодействия между ГИСЗ «МИС» и Поставщиками информации по выделенным сетям и сети Интернет должна применяться технология виртуальных частных сетей – VPN, а также средство, позволяющее устанавливать защищённое TLS соединение между клиентом и сервером, реализованное с использованием сертифицированных шифровальных (криптографических) средств, совместимых с решениями семейства ViPNet. При осуществлении информационного обмена основными сетевыми телекоммуникационными протоколами являются протоколы семейства TCP/IP. Органом криптографической защиты информации в сети ViPNet № 934 является ГБУЗ «РМИАЦ». Орган криптографической защиты по заявкам медицинских организаций создает необходимые для подключения к ГИСЗ «МИС» связи с узлами ViPNet ГБУЗ «РМИАЦ», формирует и распространяет ключевую и справочную информацию для узлов ViPNet сети №934.

Доступ к ГИСЗ «МИС» осуществляется по согласованию с Министерством здравоохранения Республики Карелия. Включение государственных учреждений здравоохранения Республики Карелия в ViPNet сеть № 934 производится по согласованию с ГБУЗ «РМИАЦ». Доступ негосударственных организаций, участвующих в реализации территориальной программы обязательного медицинского страхования и (или) оказывающих медицинские услуги гражданам на территории Республики Карелия, фармацевтических организаций к ГИСЗ «МИС» осуществляется через межсетевое взаимодействие и предварительно согласовывается с оператором ViPNet-сети, к которой подключена организация.

1.2. Общие требования по защите информации

Оператором ГИСЗ «МИС» и Поставщиками информации обязаны быть приняты меры по защите информации, содержащейся в ГИСЗ «МИС» и ИС Поставщиков

информации в соответствии с требованиями законодательства РФ в сфере защиты информации.

Обмен конфиденциальной информацией осуществляется после принятия необходимых мер по защите указанной информации от повреждения, утраты или неправомерного раскрытия третьим лицам, распространения, предусмотренных нормативными правовыми актами Российской Федерации в области защиты информации.

Руководители Поставщиков информации назначают лиц, ответственных за внесение сведений в ГИСЗ «МИС», а также лиц, ответственных за обеспечение мер по защите информации, содержащейся в ИС своей организации.

Поставщики информации несут предусмотренную законодательством Российской Федерации ответственность за полноту, достоверность и актуальность сведений, внесенных ими в ГИСЗ «МИС».

1.3. Техническая поддержка при работе с информационными системами.

Функции технической поддержки при работе в ГИСЗ «МИС» выполняет Оператор ГИСЗ «МИС» ГБУЗ «РМИАЦ».

Обращение в техническую поддержку осуществляется одним из следующих способов:

- заявка на портале http://help.zdrav10.ru;
- электронное письмо на адрес: help@zdrav10.ru;
- в случае отсутствия возможности воспользоваться первыми двумя способами, звонок на телефонные номера (с понедельника по пятницу с 8:30 до 17:00):

  +7(964)318-90-96 (по вопросам предоставления доступа и техническим проблемам, возникающим при подключении к ресурсам ГИСЗ «МИС»),

  +7(964)318-90-78 (по вопросам функционирования программного обеспечения ГИС «МИС»).

2. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

2.1. Требования к организации подключения

Подключение Поставщиков информации к ГИСЗ «МИС» осуществляется в соответствии с:

– требованиями нормативных правовых актов Российской Федерации в сфере защиты информации;

– требованиями нормативных правовых актов, технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (ФСТЭК России, ФСБ России);

– Моделью угроз и нарушителя безопасности информации ГИСЗ «МИС» и техническим заданием на создание подсистемы обеспечения информационной безопасности ГИСЗ «МИС» согласованных установленным порядком с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации;

– требованиями настоящего Регламента.

До начала выполнения работ по подключению Поставщика информации к ГИСЗ «МИС» схема защищенного взаимодействия, планируемая к реализации, обязана быть согласована с Министерством здравоохранения Республики Карелия и ГБУЗ «РМИАЦ».

2.2. Требования к реализации защищенного взаимодействия

2.2.1. Общие требования

Для организации защищенного взаимодействия Поставщика информации с ГИСЗ «МИС» в указанных организациях обязаны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы защиты информации Внешнего объекта требованиям безопасности информации не ниже уровня/класса защищенности, установленного для подключаемой подсистемы ГИСЗ «МИС».

Для проведения работ по защите информации в ходе создания и эксплуатации внешнего объекта, взаимодействующего с ГИСЗ «МИС», при необходимости, могут быть привлечены сторонние организации, имеющие, в соответствии с требованиями законодательства РФ:

– лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, проектирования в защищенном исполнении средств и систем информатизации, установки, монтажа, средств защиты информации;

– лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

Для обеспечения защиты в ГИСЗ «МИС» функционирует комплекс средств защиты, определенный Техническим заданием на создание подсистемы обеспечения информационной безопасности ГИСЗ «МИС».

2.2.2. Допустимы четыре схемы реализации подключения Поставщика информации к ГИСЗ «МИС», в каждой из которых предусмотрено использование СКЗИ для защиты передаваемой информации, что является обязательным требованием к исполнению при осуществлении взаимодействия через открытые каналы связи (выделенную сеть и сеть Интернет):

Типовая схема №1 применяется в случаях подключения к ГИСЗ «МИС» рабочих мест Поставщика информации, функционирующих в составе защищенного сегмента локально-вычислительной сети за пределами контролируемой зоны Поставщика информации. Типовая схема №1 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №1 к настоящему Регламенту.

Типовая схема №2 применяется в случаях подключения к ГИСЗ «МИС» рабочих мест Поставщика информации, функционирующих в составе защищенного сегмента локально-вычислительной сети в пределах контролируемой зоны Поставщика информации. Типовая схема №2 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №2 к настоящему Регламенту.

Типовая схема №3 применяется в случаях подключения к ГИСЗ «МИС» отдельных рабочих мест Поставщика информации, функционирующих в составе

незащищенной локально-вычислительной сети. Типовая схема №3 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №3 к настоящему Регламенту.

Типовая схема №4 применятся в случаях подключения к ГИСЗ «МИС» мобильного АРМ Поставщика информации (планшетного компьютера, ноутбука), подключенного к незащищённым выделенным сетям связи (VLAN/IPVPN). Типовая схема №4 с указанием СЗИ, в том числе СКЗИ, представлена в Приложении №4 к настоящему Регламенту.

2.2.3. Специальные требования

Помещения Поставщика информации ГИСЗ «МИС», в которых размещаются СЗИ и СКЗИ, должны удовлетворять требованиям ТУ, ЭД на данные средства и требованиям «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с СКЗИ с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 года № 152.

Работы по установке, монтажу, запуску и первоначальной настройке СЗИ и СКЗИ должны выполняться в соответствии с требованиями ТУ и ЭД на данные средства.

Эксплуатация СЗИ и СКЗИ должна осуществляться в соответствии с организационно–технической, организационно–распорядительной и ЭД на систему защиты информации Поставщика информации ГИСЗ «МИС».

Обеспечение защиты информации в ходе эксплуатации ИС Поставщика информации ГИСЗ «МИС» осуществляется владельцем ИС в соответствии с организационно–технической, организационно–распорядительной, ЭД на систему защиты информации ИСПДн Поставщика информации и нормативно–техническими документами РФ в сфере защиты информации.

Обновления операционных систем и программного обеспечения, используемого в АРМ и любом другом сетевом узле, находящемся в защищённой сети передачи данных Поставщика информации ГИСЗ «МИС», должно осуществляться с Репозитория, расположенного в ЗСПД или локально (с диска, поставляемого с формуляром).

Не допускается:

– предоставление доступа из внешнего объекта ГИСЗ «МИС» и любого другого сетевого узла, находящегося в защищённой сети передачи данных Поставщика информации ГИСЗ «МИС», в сеть Интернет или любую другую не защищённую сеть. Например, в незащищённую локально-вычислительную сеть Поставщика информации ГИСЗ «МИС»;

– предоставление доступа из незащищённых сетей к внешнему объекту ГИСЗ «МИС» и любому другому сетевому узлу, находящемуся в защищённой сети передачи данных Поставщика информации ГИСЗ «МИС»;

– использование любых беспроводных устройств совместно с компонентами ИС Поставщика информации ГИСЗ «МИС», а также подключение ИС Поставщика информации ГИСЗ «МИС» к беспроводным сетям.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ

Поставщик информации ГИСЗ «МИС» предпринимает необходимые меры по обеспечению безопасности и реализации технических требований.

Поставщик информации ГИСЗ «МИС» предоставляет Оператору ГИСЗ «МИС» ГБУЗ «РМИАЦ» Список пользователей ГИСЗ «МИС» (далее - Список) по форме Приложения №7 к настоящему Регламенту. Список должен быть утвержден руководителем организации. В дальнейшем передача актуализированного Списка осуществляется в соответствии с пунктом 4.4.

Поставщик информации по каждому сотруднику, включенному в Список, подаёт заявку на присоединение к настоящему Регламенту и подключение к ГИСЗ «МИС» (далее – Заявка) в трех экземплярах по форме Приложения №5 к настоящему Регламенту в Министерство здравоохранения Республики Карелия. Заявка должна соответствовать требованиям настоящего Регламента. Пример заполнения Заявки представлен в Приложении №6 к настоящему Регламенту.

Министерство здравоохранения Республики Карелия рассматривает Заявку в течение 2 (двух) рабочих дней и, в случае положительного результата рассмотрения Заявки, ставит отметку об утверждении и направляет в ГБУЗ «РМИАЦ» для осуществления работ по подключению.

ГБУЗ «РМИАЦ» проводит работы по подключению сотрудника Поставщика информации к ГИСЗ «МИС» течение 3 (трёх) рабочих дней.

В случае выявления несоответствия Заявки настоящему Регламенту, Министерство здравоохранения Республики Карелия, ГБУЗ «РМИАЦ» отклоняет заявку и возвращает 1 (один) экземпляр Заявки Поставщику информации с указанием выявленных недостатков. Поставщик информации имеет право подать новую заявку после устранения выявленных недостатков.

В случае повторного представления Заявки, ГБУЗ «РМИАЦ» исполняет ее в течение 10 (десяти) календарных дней.

После выполнения работ по подключению ГБУЗ «РМИАЦ» ставит на трех экземплярах Заявки отметку о выполнении работ.

Один экземпляр Заявки остаётся на хранении в ГБУЗ «РМИАЦ». Второй экземпляр Заявки направляется Поставщику информации, третий экземпляр направляется в Министерство здравоохранения Республики Карелия.

Далее ГБУЗ «РМИАЦ» в течение 2 (двух) рабочих дней создаёт идентификатор(–ы) и пароль(–и), необходимые для работы в подключенных подсистемах ГИСЗ «МИС». Идентификатор(–ы) и пароль(–и) передаются на материальных носителях или с использованием защищенных с помощью СКЗИ каналов связи, выдаются сотрудникам Поставщика информации, ответственным за внесение сведений в ГИСЗ «МИС» под личную подпись. Ответственность за сохранение реквизитов доступа в тайне возлагается на владельца реквизитов доступа.

4. КОНТРОЛЬ РЕАЛИЗАЦИИ ПОДКЛЮЧЕНИЯ

4.1. Ответственность за соблюдение требований настоящего Регламента, обеспечение требований защиты информации Поставщика информации ГИСЗ «МИС», а также ответственность за соблюдение требований к эксплуатации СЗИ и СКЗИ в составе системы защиты информации Поставщика информации, используемых в выбранной схеме подключения, лежит на лице, ответственном за обеспечение безопасности персональных данных (в случае его отсутствия – на руководителе) Поставщика информации.

Реагирование на компьютерные инциденты осуществляется в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Обеспечение действий в нештатных ситуациях при эксплуатации ГИСЗ «МИС» и принятие мер по недопущению их повторного возникновения осуществляются в соответствии с пунктом 13.6 Приказа ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

4.2. Оператор ГИСЗ «МИС» - ГБУЗ «РМИАЦ» имеет право проводить проверки реализации схем защищенного подключения Поставщика информации к ГИСЗ «МИС». В случае выявления нарушений требований настоящего Регламента или не допуска сотрудников ГБУЗ «РМИАЦ» на территорию Поставщика информации для осуществления проверки, ГБУЗ «РМИАЦ» направляет в Министерство здравоохранения Республики Карелия запрос с предложением о немедленном отключении сегмента сети, АРМ Поставщика информации от ГИСЗ «МИС» и блокировке выданных ему идентификаторов в связи с нарушением требований настоящего Регламента.

4.3. Оператор ГИСЗ «МИС» - ГБУЗ «РМИАЦ» имеет право инициировать и проводить проверку соответствия учетных записей, созданных администраторами Поставщика информации, Спискам, поданным Поставщиком информации в ГБУЗ «РМИАЦ». В случае наличия учетных записей, не входящих в указанные Списки, учетные записи блокируются ГБУЗ «РМИАЦ».

4.4. Для контроля подключенных к ГИСЗ «МИС» сотрудников, Поставщик информации подает актуальные списки учетных записей сотрудников по форме Приложения №7 в ГБУЗ «РМИАЦ»:

- периодически 1 раз в полгода (20 ноября и 20 мая);

- в случае необходимости изменения данных;

- в случае возникновения инцидента по запросу ГБУЗ «РМИАЦ».

4.5. Не допускается:

– передача (разглашение) реквизитов доступа сотрудника Поставщика информации, подключенного к ГИСЗ «МИС», другому лицу, в том числе другому сотруднику Поставщика информации,

– использование реквизитов доступа, выданных другому сотруднику Поставщика информации.

4.6. В случае выявления любых нарушений учетные записи Поставщика информации могут быть заблокированы ГБУЗ «РМИАЦ» до момента выяснения обстоятельств, с уведомлением Поставщика информации в рамках отработки инцидента информационной безопасности.

5. ПЕРЕЧЕНЬ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

– Федеральный закон Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– Федеральный закон Российской Федерации от 21 ноября 2011 года № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации";

– Постановление Правительства Российской Федерации от 16 апреля 2012 года № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

– Постановление Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Постановление Правительства Российской Федерации от 03 февраля 2012 года № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

– Постановление Правительства РФ от 06 июля 2015 года № 676 "О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации";

– Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ от 10 июля 2014 года № 378 «Об утверждении состава 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»;

- «Инструкция 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», утвержденная приказом ФАПСИ от 13 июня 2001 года № 152;

- Постановление Правительства Российской Федерации от 08 июня 2019 года № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры»;

– Постановление Правительства Российской Федерации от 05 мая 2018 года № 555 "О единой государственной информационной системе в сфере здравоохранения";

– Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Приказ ФСТЭК России от 25 декабря 2017 года № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

– Приказ ФСБ России от 24 июля 2018 года № 367 "Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации";

– Приказ ФСБ России от 24 июля 2018 года № 368 "Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения";

– Национальный проект "Здравоохранение", утвержденный 24 декабря 2018 года президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам;

- Приказ Минздрава России от 24 декабря 2018 года № 911н "Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам и информационным системам фармацевтических организаций";

– ГОСТ Р 52636-2006 "Электронная история болезни. Общие положения";

– ГОСТ Р 51624-2000 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования";

– ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения";

– ГОСТ Р 51275-2006 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения";

– ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения";

– ГОСТ Р 51583-2014 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения";

– Национальные стандарты серии "Информатизация здоровья";

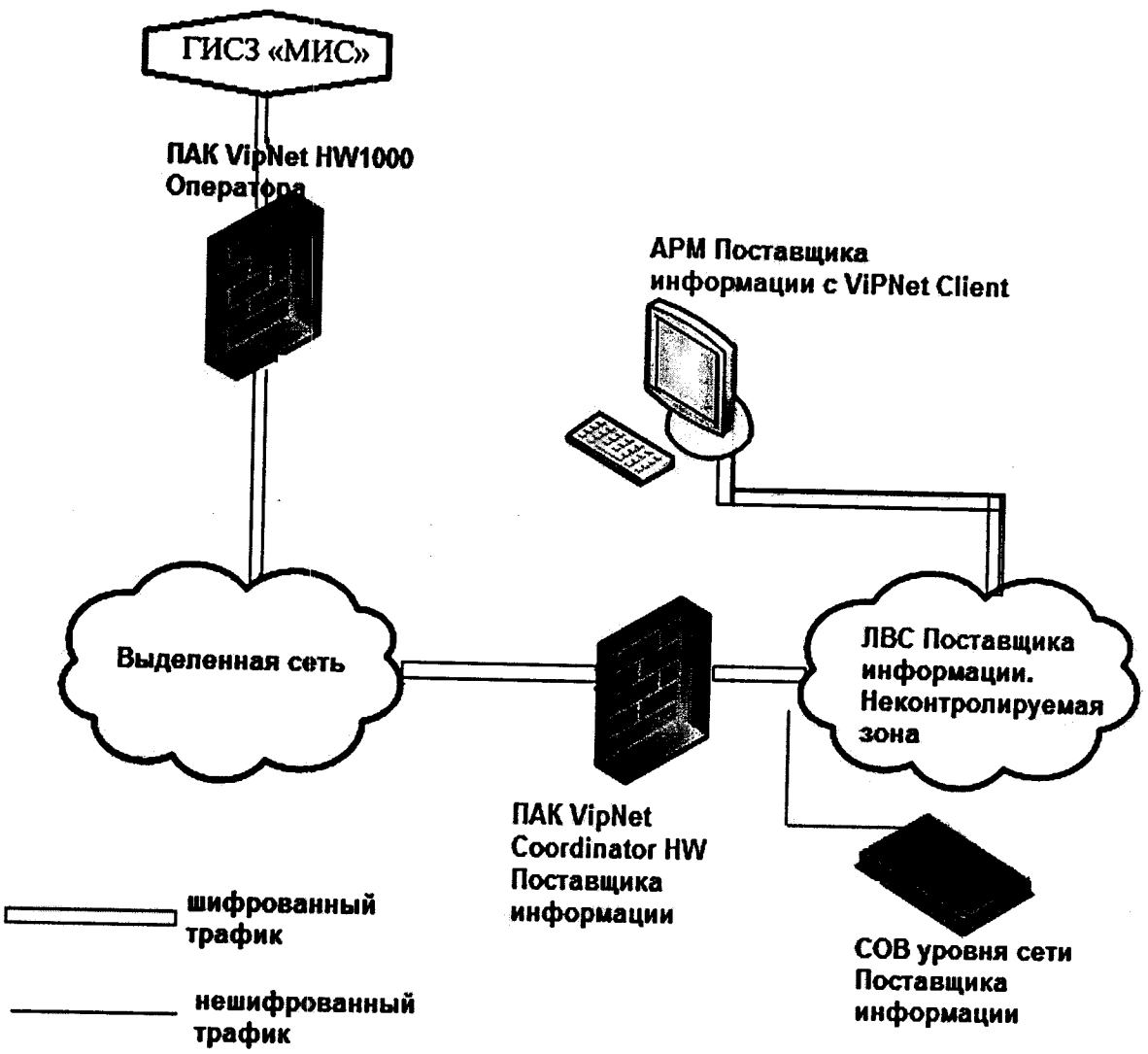
– Другие технические и методические документы ФСТЭК России и ФСБ России в области обеспечения информационной безопасности, защиты персональных данных и объектов критической информационной инфраструктуры Российской Федерации.

Приложение № 1
к Регламенту работы в ГИСЗ «МИС»

Типовая схема №1

Данная схема применятся в случаях подключения к ГИСЗ «МИС» рабочих мест Поставщика информации, размещенных за пределами контролируемой зоны Поставщика информации, но функционирующих в составе защищенного сегмента локально-вычислительной сети (например: рабочие места, находятся в защищенной ЛВС, но линии связи проходят через неконтролируемую зону, т.е. необходимо шифрование трафика внутри ЛВС).

В этом случае трафик на всем протяжении подключения должен быть зашифрован (рис. 1)



СЗИ на границе сети:

СЗИ	Рекомендуемые СЗИ	Сертификация
СКЗИ - шифрование	ПАК ViPNet Coordinator HW	сертификат ФСБ России
МЭ	ПАК ViPNet Coordinator HW	сертификат ФСБ России
СОВ уровня сети	ViPNet IDS	сертификат ФСБ России

Для обработки персональных данных Поставщика информации при подключении к ГИСЗ «МИС» должен использоваться АРМ, функционирующий в режиме ЗПС и оснащенный СЗИ:

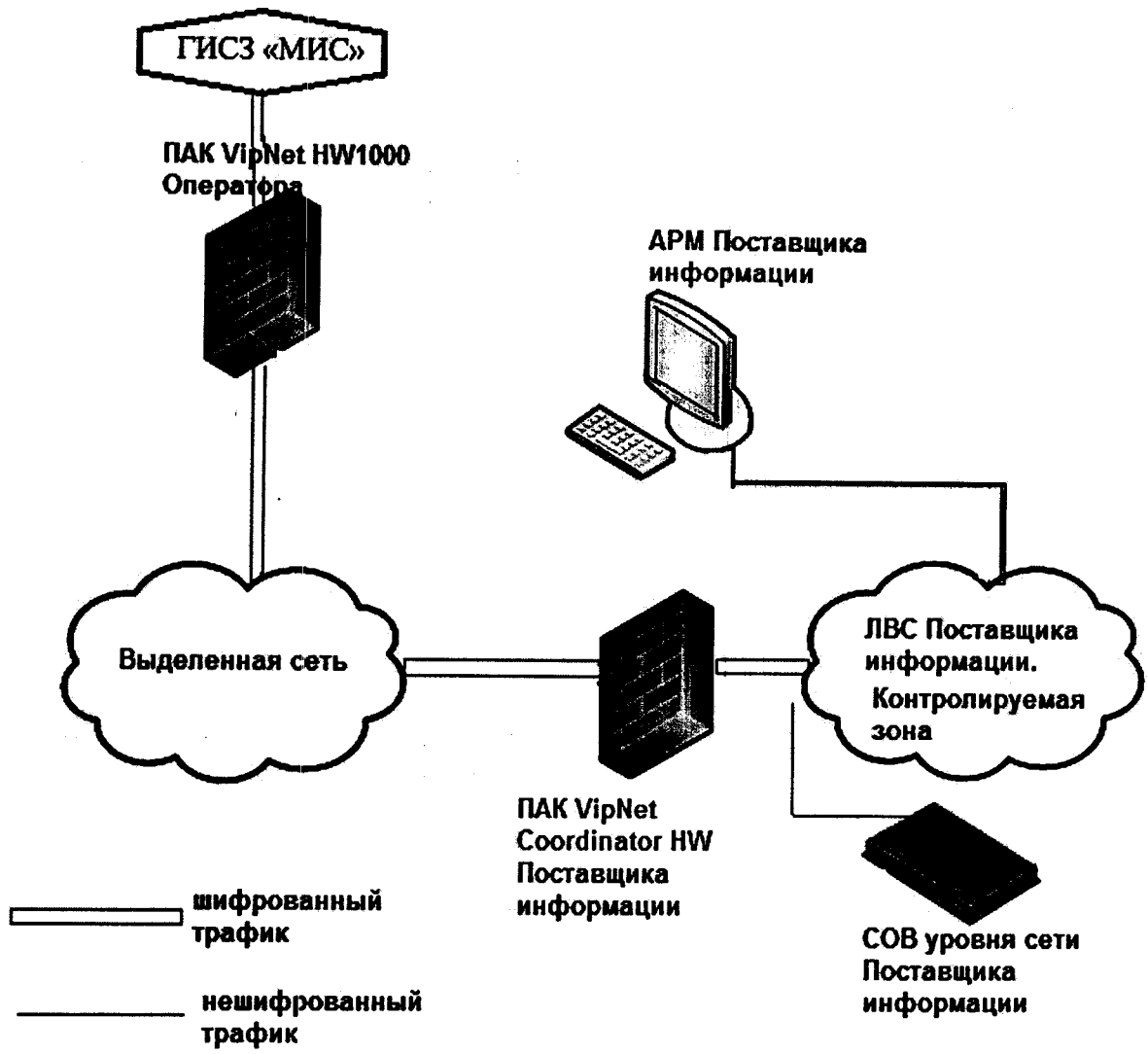
СЗИ	Рекомендуемые СЗИ	Сертификация
СЗИ от НСД	Secret Net Studio	сертификат ФСТЭК России
	встроенные СЗИ НСД операционной системы «Astra Linux Special Edition»	сертификат ФСТЭК России
СКЗИ - шифрование	ViPNet Client для индивидуального подключения АРМ пользователя или ViPNet PKI Client и браузер для доступа к веб-сервисам и возможности формирования TLS-соединения	сертификат ФСБ России
АВЗ	Kaspersky Endpoint Security для Windows	сертификат ФСТЭК России
	Kaspersky Endpoint Security для Linux	сертификат ФСТЭК России
СДЗ	программно-аппаратный комплекс «Соболь» версии 3.0 и версии 4	сертификат ФСТЭК России

Приложение № 2
к Регламенту работы в ГИСЗ «МИС»

Типовая схема №2

Данная схема применяется в случаях подключения к ГИСЗ «МИС» рабочих мест Поставщика информации, размещенных в пределах контролируемой зоны и функционирующих в составе защищенного сегмента локально-вычислительной сети Поставщика информации (например: рабочие места, находятся в защищенной ЛВС, и линии связи размещены внутри Контролируемой зоны).

В этом случае трафик должен быть зашифрован от границы контролируемой зоны Поставщика информации (рис. 2)



СЗИ на границе сети:

СЗИ	Рекомендуемые СЗИ	Сертификация
СКЗИ - шифрование	ПАК ViPNet Coordinator HW	сертификат ФСБ России
МЭ	ПАК ViPNet Coordinator HW	сертификат ФСБ России
СОВ уровня сети	ViPNet IDS	сертификат ФСБ России

Для обработки персональных данных Поставщика информации при подключении к ГИСЗ «МИС» должен использоваться АРМ, функционирующий в режиме ЗПС и оснащенный СЗИ:

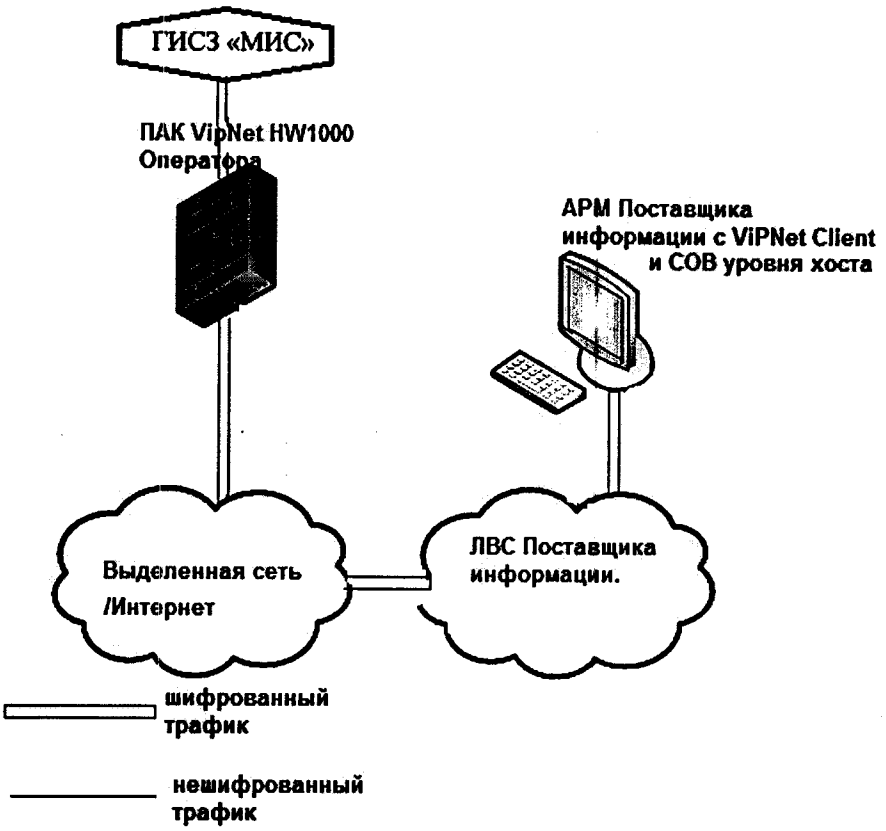
СЗИ	Рекомендуемые СЗИ	Сертификация
СЗИ от НСД	Secret Net Studio	сертификат ФСТЭК России
	встроенные СЗИ НСД операционной системы «Astra Linux Special Edition»	сертификат ФСТЭК России
АВЗ	Kaspersky Endpoint Security для Windows	сертификат ФСТЭК России
	Kaspersky Endpoint Security для Linux	сертификат ФСТЭК России
СДЗ	программно-аппаратный комплекс «Соболь» версии 3.0 и версии 4	сертификат ФСТЭК России

Приложение № 3
к Регламенту работы в ГИСЗ «МИС»

Типовая схема №3

Данная схема применяется в случаях подключения к ГИСЗ «МИС» отдельных рабочих мест Поставщика информации, функционирующих в составе незащищенной локально-вычислительной сети (Например: рабочие места, находятся в незащищенной ЛВС, а также линии связи проходят через Неконтролируемую зону).

В этом случае трафик должен быть зашифрован на всем протяжении подключения АРМ к ГИСЗ «МИС» (рис. 3)



Для обработки персональных данных Поставщика информации при подключении к ГИСЗ «МИС» должен использоваться АРМ, функционирующий в режиме ЗПС и оснащенный СЗИ:

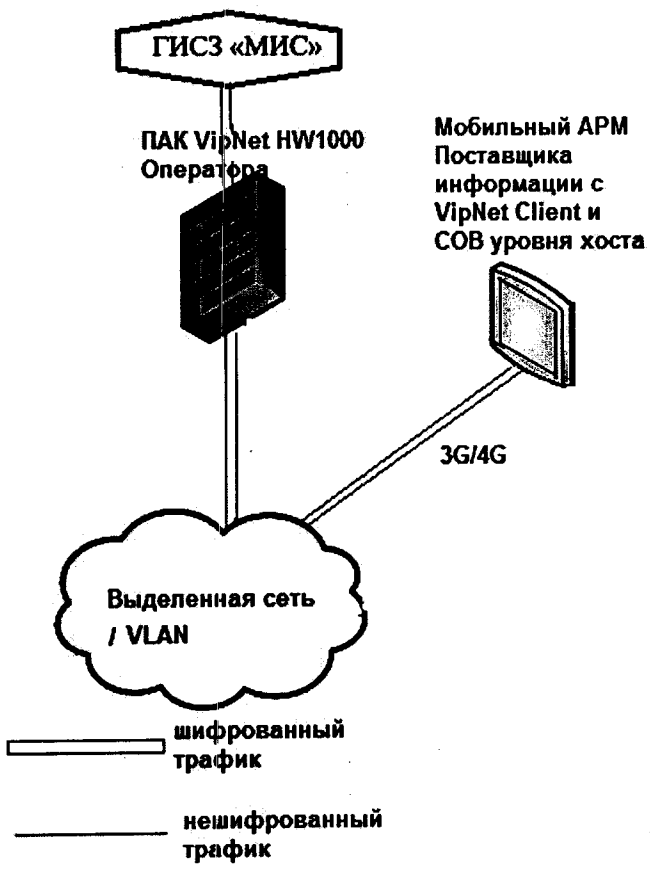
СЗИ	Рекомендуемые СЗИ	Сертификация
СЗИ от НСД	Secret Net Studio	сертификат ФСТЭК России
	встроенные СЗИ НСД операционной системы «Astra Linux Special Edition»	сертификат ФСТЭК России
СКЗИ	ViPNet Client для индивидуального подключения АРМ пользователя	сертификат ФСБ России
МЭ	встроенный МЭ СЗИ Secret Net Studio	сертификат ФСТЭК России
АВЗ	Kaspersky Endpoint Security для Windows	сертификат ФСТЭК России
	Kaspersky Endpoint Security для Linux	
СДЗ	программно-аппаратный комплекс «Соболь» версии 3.0 и версии 4	сертификат ФСТЭК России
СОВ уровня хоста	ViPNet IDS	сертификат ФСБ России

Приложение № 4
к Регламенту работы в ГИСЗ «МИС»

Типовая схема №4

Типовая схема №4 применятся в случаях подключения к ГИСЗ «МИС» мобильного АРМ Поставщика информации (планшетного компьютера, ноутбука), подключенного к незащищённым выделенным сетям связи (VLAN/IPVPN).

В этом случае трафик должен быть зашифрован на всем протяжении подключения АРМ к ГИСЗ «МИС» (рис. 4)



Для обработки персональных данных Поставщика информации при подключении к ГИСЗ «МИС» должен использоваться АРМ, функционирующий в режиме ЗПС и оснащенный СЗИ:

СЗИ	Рекомендуемые СЗИ	Сертификация
СЗИ от НСД	Secret Net Studio	сертификат ФСТЭК России
	встроенные СЗИ НСД операционной системы «Astra Linux Special Edition»	сертификат ФСТЭК России
СКЗИ	ViPNet Client для индивидуального подключения АРМ пользователя	сертификат ФСБ России
МЭ	встроенный МЭ СЗИ Secret Net Studio	сертификат ФСТЭК России
АВЗ	Kaspersky Endpoint Security для Windows	сертификат ФСТЭК России
	Kaspersky Endpoint Security для Linux	
СДЗ	Программно-аппаратный комплекс «Соболь» версии 3.0 и версии 4	сертификат ФСТЭК России
СОВ уровня хоста	ViPNet IDS	сертификат ФСБ России

Приложение № 5
к Регламенту работы в ГИСЗ «МИС»

**Заявка на присоединение к Регламенту работы в ГИСЗ «МИС»
и подключение к ГИСЗ «МИС»**

Наименование организации			
ИНН/ОГРН			
Наименование подключаемых ИСПДн/АРМов			
Номер используемой схемы подключения			
Адрес точки подключения			
ID ViPNet координатора (при наличии VipNet координатора)			
ID ViPNet Клиента подлежащего подключению (при наличии VipNet Клиента)			
IP–адреса АРМ подлежащих подключению			
ФИО, должности сотрудников, допущенных к работе с ГИСЗ «МИС»		Полномочия	
ФИО, должность сотрудника ответственного за обеспечение мер по защите информации			
Средство от НСД		Номер и срок действия сертификата соответствия	
Межсетевой экран		Номер и срок действия сертификата соответствия	
Средство антивирусной защиты		Номер и срок действия сертификата соответствия	
СКЗИ		Номер и срок действия сертификата соответствия	
Система обнаружения вторжений		Номер и срок действия сертификата соответствия	
Средство доверенной загрузки		Номер и срок действия сертификата	

		соответствия	
Наличие аттестата соответствия		Номер и срок действия аттестата, кем выдан	

Прошу подключить к ГИСЗ «МИС» АРМ в соответствии с вышеуказанной информацией и на условиях согласно Регламента работы в ГИСЗ «МИС».

Все необходимые меры по обеспечению безопасности приняты. Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ выполнены в соответствии с требованиями ТУ и ЭД на данные средства.

СКЗИ установлены в помещении, отвечающем требованиям «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 года № 152.

Сертификаты на СЗИ, в том числе СКЗИ, действительны на момент подписания Заявки. Обязанность по поддержанию системы защиты в актуальном состоянии возложена на ответственного за обеспечение мер по защите информации. В случае изменения информации, указанной в настоящей заявке, организация–заявитель обязуется сообщить об изменениях путем подачи новой заявки.

Должность:_____

_____/_____

ФИО Подпись

«____» _____202__г

МП

Отметка Министерства здравоохранения Республики Карелия

Заявка отклонена: Причина отказа:	Заявка утверждена: Должность:_____ ФИО:_____ Подпись:_____ «____» _____202__г МП

Отметка ГБУЗ «РМИАЦ»

Заявка отклонена: Причина отказа:	Работы по подключению выполнены: Должность:_____ ФИО:_____ Подпись:_____ «____» _____202__г МП

Приложение № 6
к Регламенту работы в ГИСЗ «МИС»

**Заявка на присоединение к Регламенту работы в ГИСЗ «МИС»
и подключение к ГИСЗ «МИС»
(пример заполнения)**

Наименование организации	ГБУЗ РК «ЗДОРОВЬЕ»		
ИНН/ОГРН	1234567890/1234567890123		
Наименование подключаемых ИСПДн/АРМов	АРМ Врача-терапевта		
Номер используемой схемы подключения	Схема № 2		
Адрес точки подключения	185000, г.Петрозаводск, ул. Вымышленная, дом 1, серверная		
ID ViPNet координатора (при наличии VipNet координатора)	Координатор 03A60777 СМ ЗДОРОВЬЕ (VPN № 934)		
ID ViPNet Клиента подлежащего подключению (при наличии VipNet Клиента)	-		
IP–адрес АРМ подлежащего подключению	172.16.35.77		
ФИО, должности сотрудников, допущенных к работе с ГИСЗ «МИС»	Иванов Иван Иванович, специалист	Полномочия	Пользователь подсистемы «Промед» ГИЗС «МИС»
ФИО, должность сотрудника ответственного за обеспечение мер по защите информации	Петров Петр Петрович, Администратор безопасности		
Средство от НСД	Secret Net Studio 8	Номер и срок действия сертификата соответствия	ФСТЭК России №3745 До 16.05.2025
Межсетевой экран	Программно-аппаратный комплекс ViPNet Coordinator HW 4	Номер и срок действия сертификата соответствия	ФСБ России № СФ/525-3813 До 20.12.2022 ФСТЭК России № 3692 До 26.01.2025
Средство антивирусной защиты	Kaspersky Endpoint Security 11 для Windows	Номер и срок действия сертификата соответствия	ФСТЭК России №4068 До 25.01.2024
СКЗИ	Программно-аппаратный комплекс ViPNet Coordinator HW 4	Номер и срок действия сертификата соответствия	ФСБ России № СФ/124- 4156 До 01.06.2024
Система обнаружения	VipNet IDS	Номер и срок	ФСТЭК России

компьютерных атак (вторжений) VIPNet IDS 3		действия сертификата соответствия	№4329 до 24.11.2025; ФСБ России № СФ/СЗИ-0476 до 30.06.2023
Средство доверенной загрузки	программно-аппаратный комплекс «Соболь». Версия 3.0	Номер и срок действия сертификата соответствия	ФСТЭК России №1967 До 07.12.2023
Наличие аттестата соответствия	Есть	Номер и срок действия аттестата, кем выдан	№1234/Г, действителен до 01.05.2023, ООО “Инфолайн»

Прошу подключить к ГИСЗ «МИС» АРМ в соответствии с вышеуказанной информацией и на условиях согласно Регламента работы в ГИСЗ «МИС».

Все необходимые меры по обеспечению безопасности приняты. Работы по установке, монтажу, запуску и первоначальной настройке средств защиты информации и СКЗИ выполнены в соответствии с требованиями ТУ и ЭД на данные средства.

СКЗИ установлены в помещении, отвечающем требованиям «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденной приказом ФАПСИ от 13 июня 2001 года № 152;

Сертификаты на СЗИ, в том числе СКЗИ, действительны на момент подписания Заявки. Обязанность по поддержанию системы защиты в актуальном состоянии возложена на ответственного за обеспечение мер по защите информации. В случае изменения информации, указанной в настоящей заявке, организация–заявитель обязуется сообщить об изменениях путем подачи новой заявки.

Должность: Директор ГБУЗ РК «ЗДОРОВЬЕ»

Тургенев А.В. /_____

ФИО Подпись

«01» декабря 2021г

МП

Отметка Министерства здравоохранения Республики Карелия

Заявка отклонена: Причина отказа:	Заявка утверждена: Должность:_____ ФИО:_____ Подпись:_____ «___» _____202__г МП

Отметка ГБУЗ «РМИАЦ»

Заявка отклонена: Причина отказа:	Работы по подключению выполнены: Должность:_____ ФИО:_____ Подпись:_____ «___» _____202__г МП

Приложение № 7
к Регламенту работы в ГИСЗ «МИС»

УТВЕРЖДАЮ

Главный врач ГБУЗ/Руководитель/Директор_____

_____

«____»_____202__ г.

Список пользователей

Государственной информационной системы в сфере здравоохранения Республики Карелия «Медицинские информационные системы»

«_____»

(Полное наименование Поставщика информации)

№ п/п	ФИО пользователя	IP-адрес рабочего места или ID Vipnet Client	Перечень АРМ пользователя в ГИСЗ «МИС»	Группы пользователя в ГИСЗ «МИС» (Права доступа)
1	2	3	4	5