П Р А В И Т Е Л Ь С Т В О М О С К В Ы

М О С К О В С К И Й Г О Р О Д С К О Й Ф О Н Д
О Б Я З А Т Е Л Ь Н О Г О М Е Д И Ц И Н С К О Г О С Т Р А Х О В А Н И Я

территориальный фонд обязательного медицинского страхования города Москвы

ПРИКАЗ № 497 от 15.12.2017

Об утверждении ОТТ для подключения участников информационного взаимодействия к ИР АИС ОМС

В целях выполнения требований Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в российской Федерации», Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа ФСБ России от 10.07.2014 № 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», для обеспечения защиты персональных данных в МГФОМС

ПРИКАЗЫВАЮ:

1. Утвердить Организационно-технические требования для подключения участников информационного взаимодействия к информационным ресурсам АИС ОМС (Приложение к приказу).
2. Признать утратившим силу приказ МГФОМС от 07.07.2016 № 242 «Об утверждении организационно-технических требований по подключению медицинских организаций к информационным ресурсам автоматизированной информационной системы обязательного медицинского страхования г. Москвы».
3. Контроль за исполнением настоящего приказа возложить на заместителя директора – начальника Управления информационного обеспечения системы ОМС Михеева И.А.

Директор **В.А. Зеленский**

2742

Приложение к приказу МГФОМС
№ 497 от «15» 12 2017 г.

Организационно-технические требования для подключения участников информационного взаимодействия к информационным ресурсам АИС ОМС

1. Общие положения

Московский городской фонд обязательного медицинского страхования (далее – МГФОМС) осуществляет свою деятельность в соответствии с Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, нормативными правовыми актами федерального органа исполнительной власти, осуществляющего функции по выработке государственной политики и нормативно-правовому регулированию в сфере здравоохранения, Положением об МГФОМС и нормативными правовыми актами города Москвы.

В МГФОМС создана и введена в действие автоматизированная информационная система обязательного медицинского страхования (далее – АИС ОМС), в соответствии с «Комплексной программой оптимизации деятельности Московской городской системы ОМС на 1998 - 2003 годы».

Организационно-технические требования (далее – ОТТ) по подключению участников и субъектов системы обязательного медицинского страхования г. Москвы (далее – система ОМС) к информационным ресурсам (далее – ИР) МГФОМС разработаны в соответствии с Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 21.11.2011 № 323 «Об основах охраны здоровья граждан в 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», постановлением Правительства от 01.11.2012 № 1119, Указом Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания

организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказа ФСБ России от 10.07.2014 № 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», в целях реализации защищённого информационного взаимодействия участников и субъектов системы ОМС для осуществления безопасного подключения к защищаемым ИР МГФОМС.

Настоящий документ представляет собой свод законодательных и организационно-технических требований, поясняющий руководителям организаций, осуществляющих или планирующих осуществлять свою деятельность в системе ОМС, порядок организации взаимодействия участников и субъектов системы ОМС, а также типовой порядок подключения к подсистемам (сервисам) АИС ОМС. В иных случаях рассматривается вопрос разработки индивидуального технического решения с оформлением соответствующих документов (соглашение, договор).

Медицинские организации, страховые медицинские организации, территориальные фонды, собственники других (иных) информационных систем, в том числе медицинских и государственных систем, обладатели информации - являются операторами информационных систем (далее - участники информационного взаимодействия). Требования распространяются на всех участников и субъектов системы ОМС осуществляющих обработку информации, в том числе и персональных данных субъектов персональных данных. Информация подразделяется на две категории: общедоступная информация и информация, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Обработка, предоставление и распространение информации с применением информационных технологий, информационно-телекоммуникационных сетей, информационных и автоматизированных систем (далее – ИС/АС), медицинских информационных систем (далее - МИС), производится участниками информационного взаимодействия с учетом обязательного выполнения и соблюдения требований законодательства Российской Федерации в области обеспечения безопасности информации при их обработке в ИС/АС/МИС.

Локальные нормативные акты в области обеспечения безопасности информации разрабатываются участниками информационного взаимодействия (операторами) самостоятельно.

В соответствии с требованиями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», МГФОМС, как оператор и обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.

2. Требования федерального законодательства в отношении операторов информационных систем

Во исполнение требований статьи 43 и 44 Федерального закона от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», в МГФОМС ведется персонифицированный учет сведений о застрахованных лицах и о медицинской помощи, оказанной застрахованным лицам. Порядок ведения персонифицированного учета утвержден Приказом Министерства здравоохранения и социального развития Российской Федерации от 25.01.2011 № 29н. ***Сведения о застрахованном лице и об оказанной ему медицинской помощи относятся к информации ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.***

При ведении персонифицированного учета сведений о застрахованных лицах и сведений об оказанной им медицинской помощи, участниками информационного взаимодействия (операторами) осуществляются сбор, обработка, передача и хранение данных сведений. Информация о застрахованном лице и об оказанной ему медицинской помощи относится к информации ограниченного доступа и подлежит защите в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»), Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Во исполнение требований статьи 22 и 23 Федерального закона «О персональных данных» участники информационного взаимодействия (операторы) **до начала обработки персональных данных**, обязаны уведомить уполномоченный орган по защите прав субъектов персональных

данных о своем намерении осуществлять обработку персональных данных субъектов персональных данных (застрахованных в системе ОМС), пройти регистрацию в Роскомнадзоре и получить регистрационный номер в реестре операторов персональных данных. В случае изменения сведений об опраторе, а также в случае прекращения обработки персональных данных оператор обязан уведомить об этом уполномоченный орган по защите прав субъектов персональных данных в течение десяти рабочих дней с даты возникновения таких изменений или с даты прекращения обработки персональных данных.

Используемые (разрабатываемые, внедряемые) аппаратно-программные компоненты (средства), программное и прикладное программное обеспечение, в составе ИС/АС/МИС участников информационного взаимодействия (операторов), должны быть совместимы с аппаратно-программными компонентами АИС ОМС и сетевой IT инфраструктурой МГФОМС (предусматривается руководителями организаций на этапе проектирования своих (подведомственных) ИС/АС/МИС).

Во исполнение требований статьи 18, 19 и 22 Федерального закона «О персональных данных» участник информационного взаимодействия (оператор) обязан предусмотреть в процессе своей работы (деятельности) и выполнить следующие действия:

1. назначить ответственного за организацию обработки персональных данных;
2. произвести обследование информационной системы организации, определить угрозы безопасности персональных данных при их обработке в информационной системе персональных данных;
3. определить угрозы и нарушителей безопасности информации при их обработке в информационной системе (разработать и согласовать с ФСТЭК России Модель угроз);
4. разработать и утвердить политику информационной безопасности, локальные нормативные акты (организационно-распорядительные документы) в организации для обеспечения безопасности информации;
5. определить перечень информации ограниченного доступа (персональных данных), подлежащих обработке (обрабатываемых) в информационной системе организации (оператора);
6. определить перечень лиц, доступ которым разрешен для осуществления обработки информации (персональных данных), с целью выполнения должностных (трудовых) и функциональных обязанностей;

7. установить уровень защищенности персональных данных, который необходимо обеспечивать при их обработке в информационной системе организации (с оформлением соответствующего акта о присвоении уровня защищенности);
8. реализовать комплекс организационных и технических мер по защите информации (информации ограниченного доступа, персональных данных), в соответствии с федеральными законами, положениями, нормативными и правовыми актами, методическими документами регулирующих органов в области обеспечения безопасности информации, действующие на территории Российской Федерации (при реализации технических мер защиты необходимо использовать сертифицированные средства защиты информации (далее – СЗИ) и средства криптографической защиты информации (далее - СКЗИ));
9. провести инструктаж работников (сотрудников) организации, допущенных установленным порядком к обработке информации ограниченного доступа (ПДн), довести порядок обеспечения безопасности и правила работы с СЗИ/СКЗИ;
10. организовать контроль над соблюдением условий использования и режимом эксплуатации СЗИ/СКЗИ, предусмотренных эксплуатационной, технической и проектной документацией (инструкция, инструктаж, комиссионная проверка за отчетный период, техпроект, технический паспорт, и другое);
11. организовать разбирательство и составление заключений по фактам несоблюдения условий хранения носителей защищаемой информации (ПДн), использования СЗИ/СКЗИ, которые могут привести к нарушению конфиденциальности обрабатываемой информации (ПДн) и/или другим нарушениям, которые могут привести к снижению уровня защищенности информационных систем (ПДн);
12. произвести оценку соответствия информационных систем требованиям по безопасности, разработать и принятие меры по предотвращению возможных к реализации угроз и нарушений, при необходимости предусмотреть выполнение процедуры аттестационных мероприятий на соответствие требованиям информационной безопасности (ГИС - в соответствие Требованиям приказа ФСТЭК России от 11.02.2013 № 17).

Лица, ответственные за организацию обработки и обеспечение безопасности информации в организации оператора (участника информационного взаимодействия), несут ответственность, в случаях:

- разглашения сведений, составляющих конфиденциальную информацию (информацию ограниченного доступа, ПДн) ставших ему известной в связи с исполнением должностных обязанностей;
- неисполнения или ненадлежащего исполнения своих обязанностей во исполнение требований должностных инструкций;
- непринятия своевременных мер по выявлению и пресечению нарушений требований по обеспечению информационной безопасности.

Нарушение требований в области обеспечения безопасности (защиты) информации доступ к которой ограничен, является основанием для применения дисциплинарных и административных взысканий, привлечения к уголовной ответственности, в соответствии с действующим законодательством Российской Федерации.

В соответствии с частью 2 статьи 3 Федерального закона «О персональных данных» МГФОМС является оператором. МГФОМС, как оператор имеет право самостоятельно определять состав, и перечень мер, необходимых и достаточных для выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

3. Описание основных принципов и мероприятий по организации взаимодействия с ИР АИС ОМС

В составе АИС ОМС функционируют различные специализированные информационные подсистемы (сервисы) обрабатывающие информацию ограниченного доступа, такие как: Персонифицированный учет медицинской помощи (далее - ПУМП), Региональный сегмент Единого регистра застрахованных лиц (далее - РС ЕРЗЛ), Медико-социологическая интегрирующая система (далее - МСИС), Единый информационный ресурс учета свободного коечного фонда и госпитализации (далее – ЕИРКГ), и другие.

Для организации защищенного информационного обмена данными участникам информационного взаимодействия (операторам) необходимо знать:

1. Номер защищенной сети МГФОМС - **394**.

2. ***Доступ к защищаемым ИР АИС ОМС осуществляется по факту письменного подтверждения участником информационного взаимодействия (оператором) выполнения требований федерального законодательства в области обеспечения безопасности информации при её обработке в ИС/АС/МИС, с учетом ОТТ.***
3. Доступ к подсистемам (сервисам) осуществляется с применением определенных правил (на чтение/запись/обновление), которые устанавливаются и контролируются администраторами подсистем (сервисов) АИС ОМС в МГФОМС.
4. Дополнительные (специализированные, локальные, автоматические, автоматизированные, и другие) функции для организации обработки информации в составе ИС/АС/МИС, не являющиеся основной задачей защищенного информационного взаимодействия в АИС ОМС, но необходимые для её распространения, в целях оказания медицинской помощи в организациях с учетом требований законодательства Российской Федерации, разрабатываются и внедряются участником информационного взаимодействия (оператором) самостоятельно.
5. Размещение, установка и настройка программно-аппаратных комплексов и программного обеспечения СЗИ/СКЗИ должны производится оператором в соответствие требованиям эксплуатационной документации разработчика. Настройка ПО/ППО/СЗИ/СКЗИ производится работниками (специалистами) участников информационного взаимодействия (операторами) самостоятельно и/или с привлечением специализированных организаций (специалистов) в данной области, на усмотрение руководителя организации (оператора) подключаемой ИС/АС/МИС.
6. Независимо от приведенных ниже вариантов подключения ИС/АС/МИС к ИР АИС ОМС, участник информационного взаимодействия (оператор) обязан организовать подключение одного АРМ (минимум) для оператора ввода данных по схеме № 1. Это необходимо для осуществления доступа к сервисам подсистем в режиме «реального времени», а также защищенного обмена информацией (электронными сообщениями/ документами) между операторами ввода данных участников информационного взаимодействия (операторов).
7. Установление защищенного канала реализуется следующими способами:

1) применением автоматизированного рабочего места оператора ввода данных (далее – АРМ) через веб-интерфейс в режиме «реального времени»;
2) применением ИС/АС/МИС для обращения к сервисам АИС ОМС;
3) организацией межсетевого взаимодействия между защищенными сетями участников информационного обмена (операторами информационных систем). Осуществляется с применением технологии ViPNet. Основанием является, заключаемое Сторонами обмена, Соглашение об организации защищенного межсетевого взаимодействия (Приложение № 4 к ОТТ).

8. Для обеспечения интеграции МИС с ИР АИС ОМС участникам информационного взаимодействия (операторам) необходимо выполнить:
   1) ***требования законодательства Российской Федерации, нормативных документов федеральных органов исполнительной власти, уполномоченных на деятельность по защите информации, действующих стандартов в области применения информационных технологий и защиты информации***;
   2) требования регламента информационного взаимодействия участников ОМС г. Москвы в АИС ОМС (информация доступна на сайте МГФОМС, в разделе «Документы» - «Нормативная база»);
   3) доработку МИС в соответствии с требованиями технической документации (информация доступна на сайте МГФОМС, в разделе «Документы» - «Нормативная база»).

4. Описание организации защищенного доступа АРМ оператора к ИР АИС ОМС

4.1 Требования к АРМ

АРМ оператора ввода данных для работы в ИР АИС ОМС (МГФОМС), с целью обработки информации доступ к которой ограничен федеральным законодательством (информация ограниченного доступа, сведения конфиденциального характера, ПДн) должны размещаться в пределах контролируемой зоны (далее – КЗ). Организационно-технические мероприятия, выполняемые участниками и субъектами системы ОМС для обеспечения организации КЗ, должны исключать возможность неконтролируемого проникновения и/или пребывания посторонних лиц в её пределах. Такие помещения и перечень лиц, допущенных для работы в них, рекомендуется определять приказом по организации.

Рекомендуемые к реализации технические требования к АРМ:

№	Наименование параметра	Техническая характеристика
1.	Процессор	Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более
2.	Объем оперативной	Не менее 2 Гбайт (рекомендуется 4 Гб и более)
3.	Свободное место на жестком диске	Не менее 300 Мбайт
4.	Сетевое оборудование	Наличие сетевого адаптера или модема
5.	Дисплей	Минимальное разрешение экрана дисплея - 1280x800 (рекомендуется - 1440x900 и выше)
6.	Операционная система	Windows 7 (32/64-разрядная)
7.	Браузер	Microsoft Internet Explorer – версия 9.0 и выше/Mozilla Firefox – версия 33 и выше/Google Chrome - версия 28 и выше/Opera - версия 11 и выше
8.	Канал связи	Подключение к каналу сети Internet с пропускной способностью не менее 10 Мбит/с (остальное на усмотрение (ответственность) руководителя подключаемой организации)

Для обеспечения выполнения участниками и субъектами системы ОМС минимальных требований, в целях соблюдения мер по защите информации, доступ к которой ограничен в соответствии с требованиями действующего федерального законодательства на территории Российской Федерации, на АРМ должны быть установлены сертифицированные ФСТЭК и ФСБ России средства защиты информации (далее - СЗИ):

№	Наименование СЗИ	Варианты сертифицированных СЗИ
1.	Антивирусное программное обеспечение	Kaspersky Endpoint Security 8, Kaspersky Endpoint Security 10, ESET NOD32 Secure Enterprise Pack (версия 5.0), Dr.Web Enterprise Security Suite и др.
2.	Средство защиты информации от НСД (далее – ПО/ПАК СЗИ от НСД)	Dallas Lock 8.0-К, Аккорд-Win32, Панцирь-К, Secret Net 7 и др.
3.	Средство криптографической защиты информации (далее – СКЗИ) (При организации подключения АРМ оператора по Схеме №1.2 см. ниже)	Необходимо использовать сертифицированные версии ПО ViPNet Client (на момент выхода документа - версии 4 и 3.2).

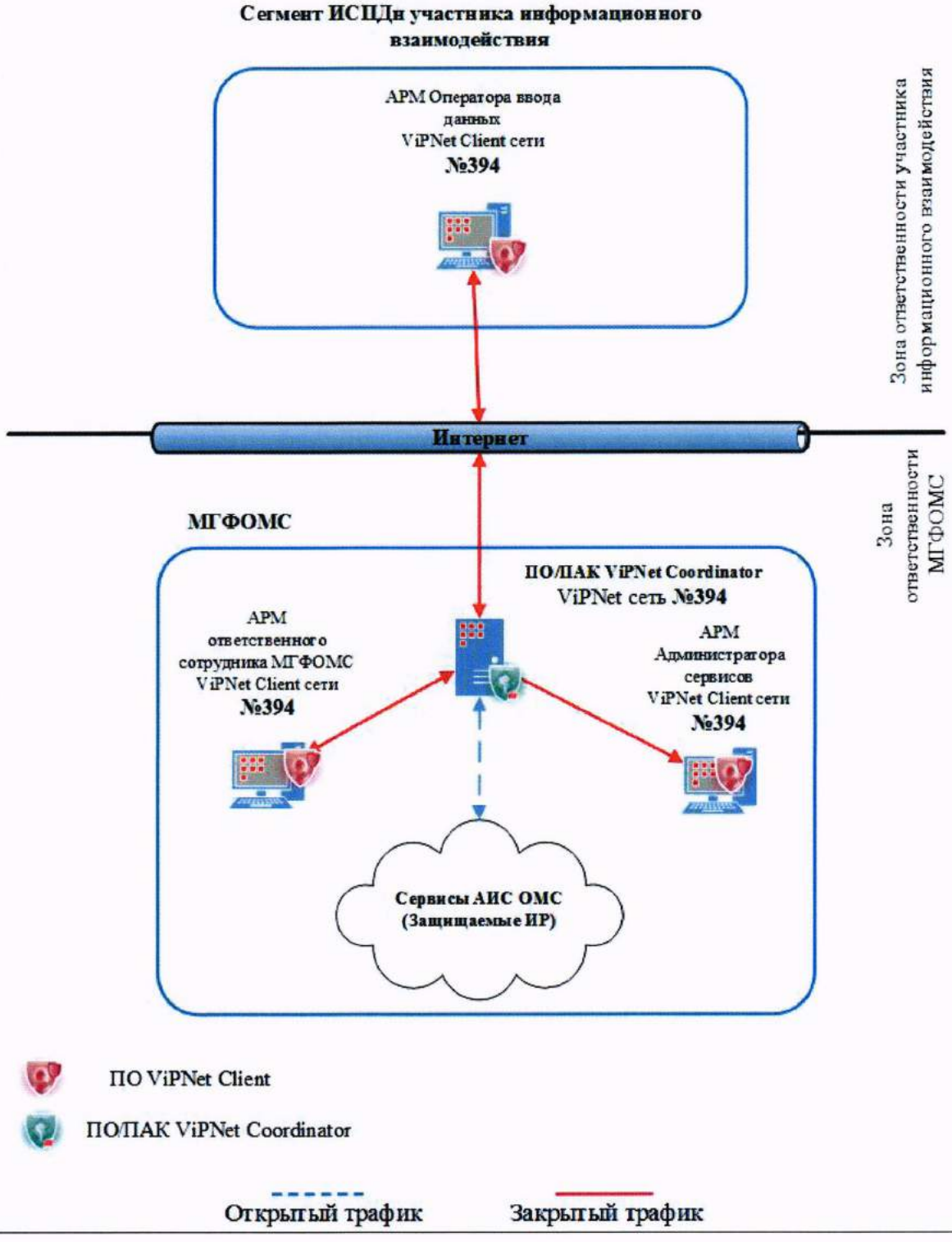
4.2 Организация защищенного подключения АРМ к ИР АИС ОМС (схема №1)

При организации подключения АРМ оператора по Схеме №1:

- На все АРМ, которые будут обращаться к ИР АИС ОМС, операторам необходимо самостоятельно и за свой счет, приобрести и установить сертифицированные СЗИ (минимальный набор средств для установки состоит из: ПО ViPNet Client, антивирусного ПО и ПО или ПАК СЗИ от НСД).
- Дальнейшие действия оператора указаны в Приложении № 1 к ОТТ.

Схема №1

Организация защищенного канала для передачи данных между участником информационного взаимодействия и сервисами АИС ОМС с применением АРМ



5. Описание организации защищенного доступа ИС/АС/МИС к ИР АИС ОМС

Участники информационного взаимодействия самостоятельно проектируют и осуществляют внедрение своих (ведомственных) ИС, которые могут функционировать под управлением различных операционных систем (далее - ОС), приобретенных официально у производителя. Сервер может иметь различные рабочие характеристики и исполнение.

Руководителям участников информационного взаимодействия (операторам) необходимо выполнять требования по построению информационных систем в защищенном исполнении, а также систем защиты персональных данных в соответствии с требованиями законодательства Российской Федерации, нормативных документов федеральных органов исполнительной власти, уполномоченных на деятельность по защите информации, действующих стандартов в области применения информационных технологий и защиты информации (ГОСТ Р 51583, ГОСТ Р 51624, ГОСТ 34.601, ГОСТ 34.602-89).

В данном разделе изложены рекомендации по обеспечению безопасности информации при организации канала передачи данных в защищенном исполнении, используя Глобальную сеть (Интернет) для связи ИС/АС/МИС и ИР АИС ОМС. Решение об использовании выделенного канала связи (физический кабель – ВОЛС) для организации информационного взаимодействия между ИС/АС/МИС принимается операторами самостоятельно. Выполнение требований по обеспечению безопасности передаваемых данных между ИС/АС/МИС и ИР АИС ОМС обеспечивается сертифицированными средствами криптографической защиты информации. Доступ участников информационного взаимодействия и субъектов системы ОМС к ИР АИС ОМС осуществляется с использованием технологии ViPNet, в МГФОМС развернута и функционирует защищённая сеть №394. Администрирование и управление связью защищенной сети №394 осуществляет только администратор СКЗИ МГФОМС.

5.1 Требования к ИС/АС/МИС

Рекомендуемые к реализации технические требования для организации сервера ИС/АС/МИС под управлением ОС Windows:

№	Наименование параметра	Требуемая характеристика
1.	Процессор	Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более
2.	Объем оперативной памяти	От 2048 Мб доступных для ПО Infotecs
3.	Свободное место на жестком диске	Не менее 1024 Мбайт
4.	Сетевое оборудование	Наличие 2-х сетевых адаптеров
5.	Операционная система	• Windows Server 2003 (32-разрядная) • Windows Vista SP2 (32/64-разрядная) • Windows Server 2008 (32/64-разрядная) • Windows 7 (32/64-разрядная) • Windows Server 2008 R2 (64-разрядная)

Рекомендуемые к реализации технические требования для организации сервера ИС/АС/МИС под управлением ОС семейства Linux:

№	Наименование параметра	Требуемая характеристика
1.	Процессор	Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более
2.	Объем оперативной памяти	От 1024 Мб доступных для ПО Infotecs
3.	Свободное место на жестком диске	Не менее 500 Мбайт
4.	Сетевое оборудование	Наличие 2-х сетевых адаптеров

5.	Операционная система	• ALT Linux 6.0 Server; • ALT Linux 6.0 Desktop; • CentOS 5.4; • CentOS 5.7; • CentOS 6.0; • Mandriva Linux 2010 Powerpack; • RedHat Enterprise Linux 5.4; • RHEL 5.7; • RHEL 6.0 AS; • Slackware Linux 12.0 (только ядро 2.6.16.52 с FTP-сервера ftp://kernel.org); • Slackware Linux 12.2; • SUSE Linux Enterprise Server 10; • SUSE Linux Enterprise Server 10 SP1, SP2, SP3; • SUSE Linux Enterprise Server 11; • SLES 11 SP1; • Ubuntu 10.04.

Для обеспечения выполнения минимальных требований, в целях соблюдения мер по защите информации, доступ к которой ограничен в соответствии с требованиями действующего федерального законодательства, на сервер ИС/АС/МИС должны быть установлены сертифицированные ФСТЭК и ФСБ России СЗИ:

Защищаемый объект	Наименование СЗИ	Варианты сертифицированных СЗИ
Физическая машина: Сервер	Антивирусное программное обеспечение	Kaspersky Endpoint Security 8, Kaspersky Endpoint Security 10, ESET NOD32 Secure Enterprise Pack (версия 5.0), Dr.Web Enterprise Security Suite и др.
	ПО/ПАК СЗИ от НСД	Dallas Lock 8.0-К, Аккорд-Win32, Панцирь-К, Secret Net 7 и др.

	СКЗИ	Необходимо использовать сертифицированные версии ПО ViPNet Coordinator.
Средства виртуализации сервера ИС/АС/МИС	Сертифицированные средства защиты среды виртуализации	Например: vGate R2
	Антивирусное средство защиты виртуальной среды	Kaspersky Security для виртуальных сред 2.0, Kaspersky Security для виртуальных сред 3.0 Легкий агент, Symantec Endpoint Protection, ESET NOD32 Secure Enterprise и др.
	СКЗИ	Необходимо использовать сертифицированные версии ПО ViPNet Coordinator.

5.2 Варианты условий организации защищенного канала для подключения ИС/АС/МИС к ИР АИС ОМС

Вариант №1 (схема №2.1)

Данный вариант подразумевает приобретение организацией (оператором) ПО ViPNet Coordinator Windows или Linux и его установку на сервер ИС/АС/МИС.

Данный вариант организации защищенного подключения, отображен на **Схеме №2.1:**

При данном варианте подключения:

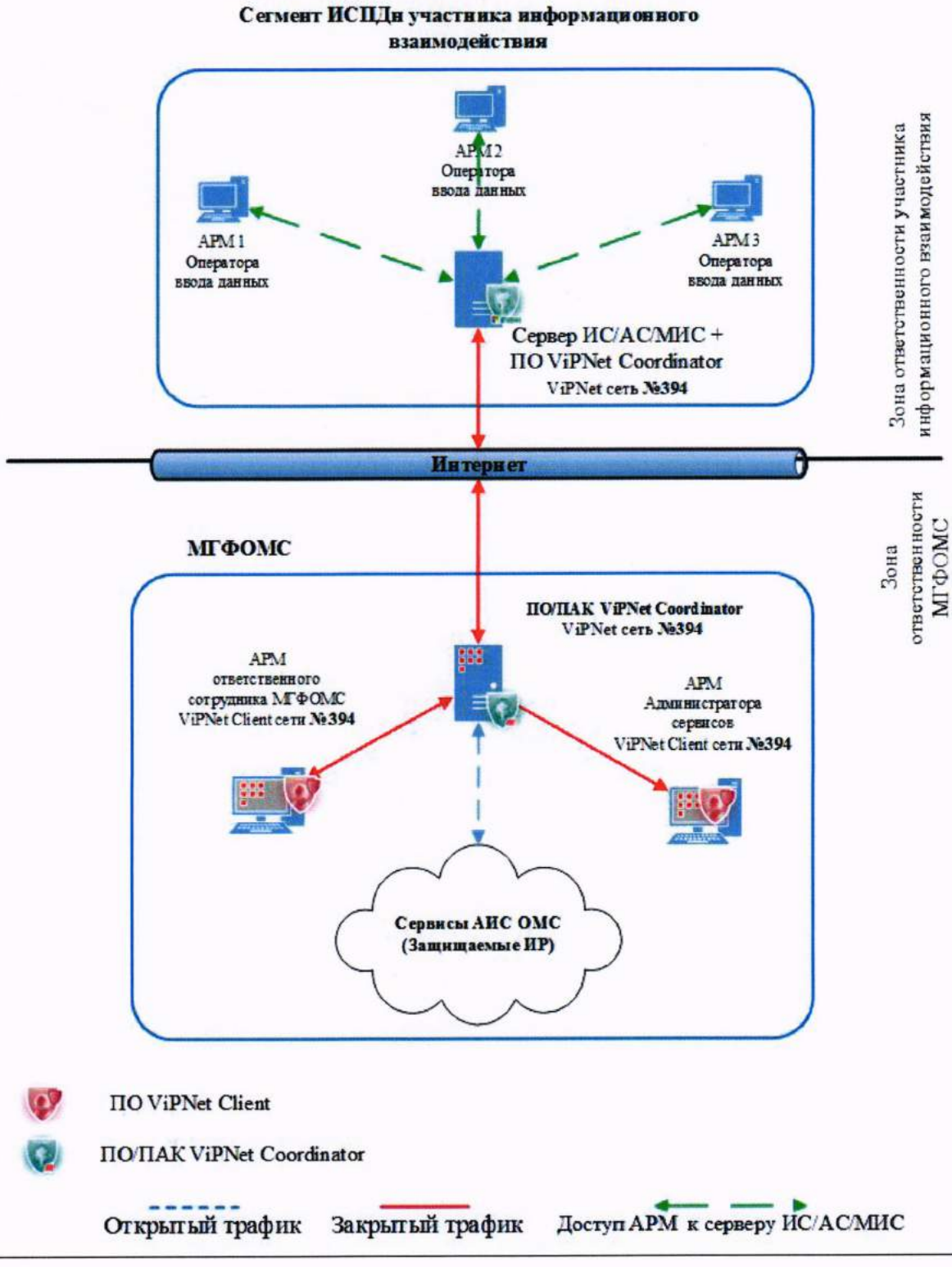
- на сервер ИС/АС/МИС необходимо самостоятельно и за свой счет, приобрести и установить сертифицированные СЗИ (ПО ViPNet Coordinator, антивирусное ПО и ПО/ПАК СЗИ от НСД).
- Дальнейшие действия оператора указаны в Приложении № 1 к ОТТ.
- По окончанию работ, предписанных в Приложении № 1 к ОТТ настоящего документа, совместно с администратором защищенной сети МГФОМС прописать необходимые для установления защищенного канала правила фильтрации в ПО ViPNet Coordinator, установленного на сервере ИС/АС/МИС. Для этого, необходимо предварительно сообщить администратору защищенной сети МГФОМС IP-адреса (диапазон IP-

адресов) АРМ пользователей ИС/АС/МИС (указать данную информацию необходимо на этапе оформления Заявки для подключения участника информационного взаимодействия к ИР АИС ОМС).

Обращаем Ваше внимание на то, что доступ пользователей оператора к ресурсам ИС/АС/МИС организации может быть невозможен в процессе установки на сервер ИС/АС/МИС ПО ViPNet Coordinator до момента его переконфигурации (завершения инсталляции). Необходимо не допускать ошибок при заполнении Заявки на подключение участника информационного взаимодействия к ИР АИС ОМС и не нарушать порядок работ, описанных в переданной ответственному представителю организации инструкции.

Схема №2.1

Организация защищенного канала для передачи данных между участником информационного взаимодействия и сервисами АИС ОМС с применением ИС/АС/МИС



Вариант №2 (схема №2.2)

Данный вариант подразумевает приобретение и установку организацией (оператором) ПО/ПАК ViPNet Coordinator:

1. ПО ViPNet Coordinator;
2. HW100 (пропускная способность не выше 20 Мбит/сек);
3. HW1000 (пропускная способность не выше 280 Мбит/сек).

Для обеспечения выполнения минимальных требований, в целях соблюдения мер по защите информации, доступ к которой ограничен в соответствии с требованиями действующего федерального законодательства, на сервер ИС/АС/МИС должны быть установлены сертифицированные ФСТЭК и ФСБ России СЗИ:

Защищаемый объект	Наименование СЗИ	Варианты сертифицированных СЗИ
Физическая машина: Сервер	Антивирусное программное обеспечение	Kaspersky Endpoint Security 8, Kaspersky Endpoint Security 10, ESET NOD32 Secure Enterprise Pack (версия 5.0), Dr.Web Enterprise Security Suite и др.
	ПО/ПАК СЗИ от НСД	Dallas Lock 8.0-К, Аккорд-Win32, Панцирь-К, Secret Net 7 и др.
Средства виртуализации сервера МИС	Сертифицированные средства защиты среды виртуализации	Например: vGate R2
	Антивирусное средство защиты виртуальной среды	Kaspersky Security для виртуальных сред 2.0, Kaspersky Security для виртуальных сред 3.0 Легкий агент, Symantec Endpoint Protection, ESET NOD32 Secure Enterprise и др.

Данный вариант организации защищенного подключения, отображен на **Схеме №2.2**. При организации подключения дальнейшие действия оператора указаны в Приложении № 1 к ОТТ.

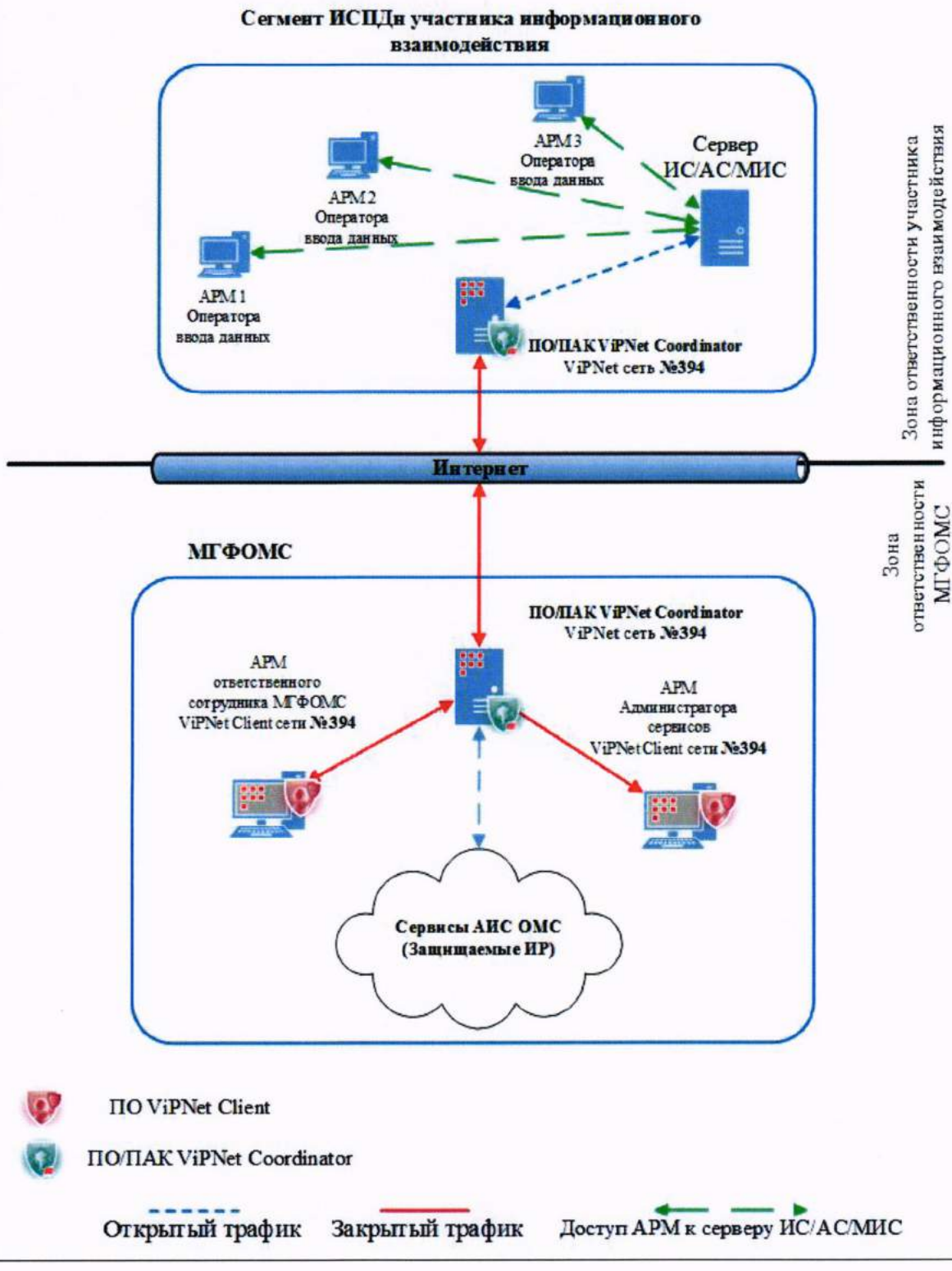
По завершению работ, предписанных в Приложении № 1 к ОТТ настоящего документа, присвоить серверу ИС/АС/МИС IP-адрес, выделенный при выдаче ключевой информации администратором

защищенной сети МГФОМС №394, произвести необходимые работы по настройке маршрутизации на сервере ИС/АС/МИС для его дальнейшего взаимодействия с ПО/ПАК ViPNet Coordinator, внутренний IP-адрес которого также выделяется при выдаче ключевой информации в МГФОМС.

Необходимо не допускать ошибок при заполнении заявки на подключение участника информационного взаимодействия к ИР АИС ОМС и не нарушать порядок работ, описанных в переданной ответственному представителю организации инструкции.

Схема №2.2

Организация защищенного канала для передачи данных между участником информационного взаимодействия и сервисами АИС ОМС с применением ИС/АС/МИС



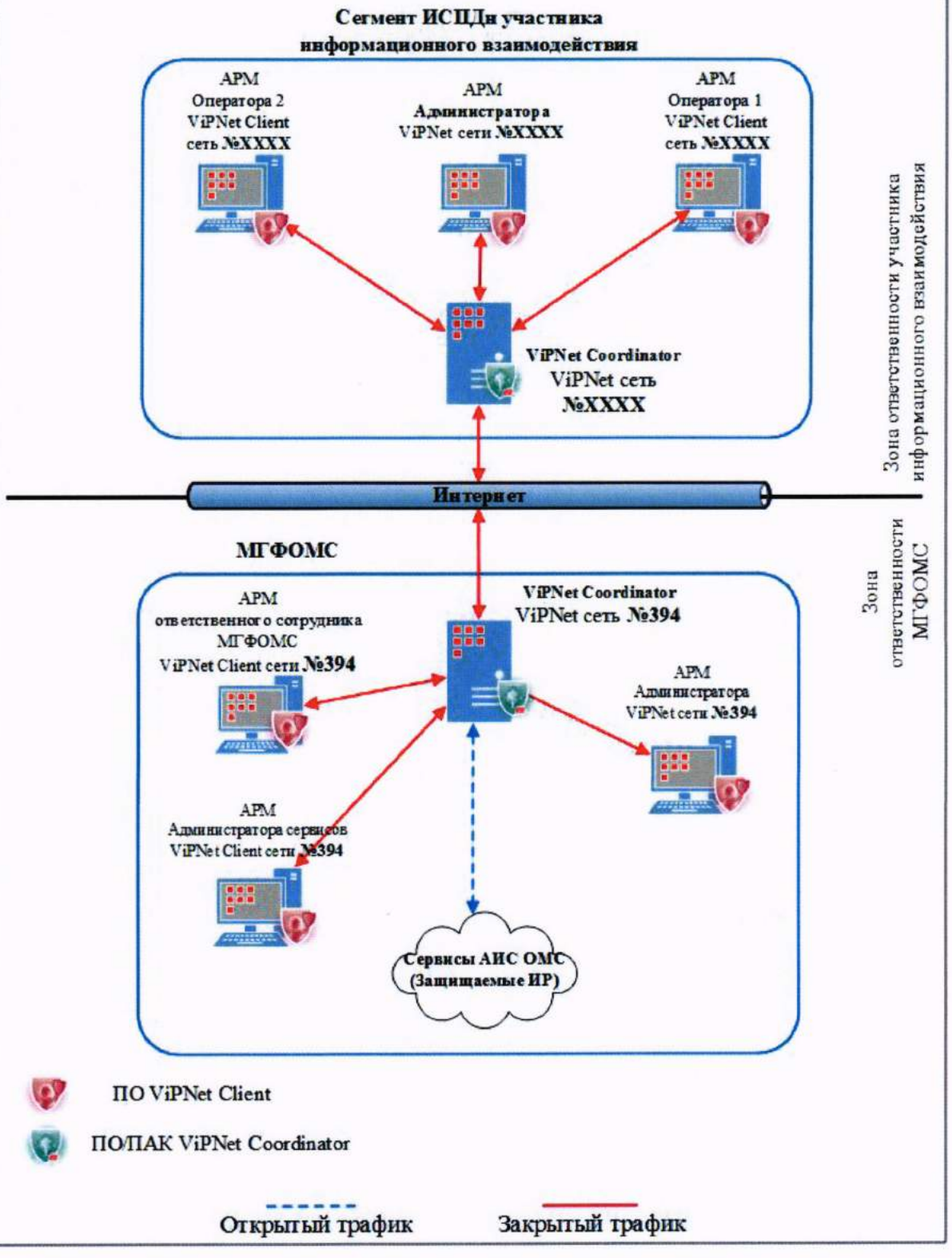
6 Описание организации защищенного межсетевого взаимодействия с применением технологии ViPNet

Для организации защищенного межсетевого взаимодействия с применением технологии ViPNet между защищенными сетями участников информационного взаимодействия и МГФОМС необходимо обоснование для организации такого подключения. По факту принятия решения о целесообразности организации межсетевого взаимодействия между участниками информационного обмена заключается Соглашение об организации защищенного информационного взаимодействия. После заключения Соглашения и выполнения работ, прописанных в Приложении № 1 к ОТТ настоящего документа, участникам необходимо выполнить установленный производителем порядок действий для организации межсетевого взаимодействия, описанный в эксплуатационной документации на ПО Administrator.

Данный вариант организации защищенного подключения, отображен на **Схеме №3.**

Схема №3

Реализуется при организации защищенного межсетевого взаимодействия ViPNet Сетей между участником информационного взаимодействия и сервисами АИС ОМС



Приложение № 1 к ОТТ

Описание процедуры организационного взаимодействия между участниками информационного взаимодействия

Для начала выполнения работ по организации защищенного информационного взаимодействия между его участниками необходимо выполнить следующие действия:

1. Выполнить требования законодательства Российской Федерации, нормативных документов федеральных органов исполнительной власти, уполномоченных на деятельность по защите информации, действующих стандартов в области применения информационных технологий и защиты информации.
2. Обеспечить допущенных сотрудников автоматизированными рабочими местами с установленными на них сертифицированными средствами защиты.
3. Направить по электронной почте:

по адресу **oms2016@mgfoms.ru** список сотрудников для обучения работе с сервисами (подсистемами) АИС ОМС, в соответствии с Приложением № 2 к ОТТ;

4. Направить по электронной почте на адрес **secur@mgfoms.ru** полностью и корректно заполненную форму заявки на подключение участника информационного взаимодействия к ИР АИС ОМС, по установленной форме в Приложении № 3, для проверки корректности заполнения:
   4.1. Тема электронного сообщения: Заявка на подключение + название участника информационного взаимодействия;
   4.2. В тексте письма указать контактную информацию ответственного за оформление документов (ответственного за организацию и обеспечение безопасности информации (ПДн)).
   4.3. **Необходимо обратить ВНИМАНИЕ -** регистрационный номер в реестре операторов ПДн в заявке указывается в том случае, если он есть у оператора (если участник информационного взаимодействия успешно прошел регистрацию в Роскомнадзоре и зарегистрирован в реестре операторов ПДн).

   Отсутствие регистрации (регистрационного номера) в реестре операторов ПДн не является ограничением для подключения к ИР АИС ОМС (МГФОМС), но является обязанностью оператора ПДн, руководителя организации, участника информационного взаимодействия

подключённого или подключаемого к ИР АИС ОМС (статья 22 Федерального закона «О персональных данных»).

5. После получения подтверждения корректности оформления заявки на подключение участника информационного взаимодействия к ИР АИС ОМС, необходимо курьером (нарочным, почтовым отправлением (обычным/заказным)) направить письмо-уведомление о готовности к подключению и выполнении ОТТ, на имя директора МГФОМС, к нему приложить (при организации нового и/или дополнительного подключения) полностью заполненную заявку на подключение (в соответствии с ОТТ) участника информационного взаимодействия к ИР АИС ОМС.

6. Получить в МГФОМС, под роспись, справочную и методическую информацию (ключи) для установления защищенного канала и инструкцию по настройке АРМ, которые планируются к подключению в соответствии с представленной в МГФОМС заявкой. Пройти инструктаж по правилам безопасности обращения со средствами защиты информации. С собой иметь чистый CD-R/DVD-R диск. При себе иметь Паспорт гражданина РФ для осуществления санкционированного прохода в здание, через охрану.

7. В составе ИС/АС/МИС произвести необходимые настройки в соответствии с полученными инструкциями. Убедится по завершению работ в том, что защищенный канал установлен путем отправки и получения тестовых сообщений в сети ViPNet № 394, между АРМ оператора ввода данных участника информационного взаимодействия и АРМ администратора защищенной сети МГФОМС (Администратор ПОИБ АИС ОМС).