МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
КАЛИНИНГРАДСКОЙ ОБЛАСТИ

Государственное бюджетное учреждение здравоохранения
«Медицинский информационно-аналитический центр
Калининградской области»
(МИАЦ)

ПРИКАЗ

«11» июля 2018 г. № 79-О

Калининград

Об утверждении регламента защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области»

Во исполнение требований Федеральных законов от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных», приказов Федеральной службы по техническому и экспортному контролю Российской Федерации 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», от 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в целях организации работы регионального сегмента единой государственной информационной системы в сфере здравоохранения Калининградской области (далее – РС ЕГИСЗ),

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие Регламент защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области» (далее – Регламент) согласно приложению к настоящему приказу.

2. Начальнику отдела сетевых технологий и информационных ресурсов (Шишкиной Н.И.):

1) довести настоящий приказ до всех организаций, подключенных к РС ЕГИСЗ, в срок до 13 июля 2018 года;

2) организовать эксплуатацию РС ЕГИСЗ, контроль за подключением новых организаций и объектов к РС ЕГИСЗ в соответствии с Регламентом, срок весь период.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор В.В. Рыскаль

Приложение
к приказу от «11» июля 2018 № 79-О

РЕГЛАМЕНТ
защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской 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.

ViPNet [Координатор] – программное обеспечение или программно-аппаратный комплекс, 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.

Абонентский пункт – персональный компьютер или терминальная станция, подключенные к защищенной сети.

Администратор Защищенной сети – назначенный приказом директора сотрудник Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области», осуществляющий администрирование всей Защищённой сети.

Локальный администратор Защищенной сети – назначенный приказом руководителя сотрудник Участника Защищенной сети, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих Участнику Защищенной сети.

Информационная система – совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств.

Центр управления сетью – аппаратные и/или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети.

Участник Защищенной сети – организация, имеющая доступ к Защищенной сети.

Абонент – назначенный приказом руководителя сотрудник Участника Защищенной сети, использующий для выполнения своих служебных обязанностей сервисы и информационные системы Защищённой сети.

Защищённая сеть – защищённая виртуальная сеть ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области», имеющая учетный номер 763.

2. Общие положения

2.1. Регламент защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области» (далее – Регламент) разработан 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»;

– Приказом ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказом ФСБ России от 10 июля 2014 г. № 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»;

– Приказом ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

– Приказ Министерства здравоохранения Калининградской области от 09 декабря 2016 г. № 532 «О вводе в эксплуатацию государственной информационной системы «Региональный сегмент Единой государственной информационной системы в сфере здравоохранения Калининградской области».

2.2. Регламент определяет и устанавливает:

– права, обязанности и ответственность администраторов и абонентов Защищенной сети;

– порядок организации и подключения Участников Защищенной сети (далее – Участники) к защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области» (далее – Защищённая сеть);

– порядок предоставления доступа к информационным системам Защищённой сети;

– порядок организации защищённого межсетевого взаимодействия.

3. Назначение защищённой сети

Основными задачами, которые решает Защищённая сеть, являются:

– Организация защищённого информационного взаимодействия между Участниками и центрами обработки данных (далее – ЦОД), расположенными по следующим адресам:

  – 236007, г. Калининград, ул. Дмитрия Донского, д. 1;
  – 236016, г. Калининград, ул. Клиническая, д. 74;
  – 236000, г. Калининград, ул. Мусоргского, д. 74.

– Уменьшение вероятности потери, искажения и хищения информации при её передаче между Участниками и ЦОД.

– Организация защищённого доступа Участниками к информационным ресурсам, в целях реализации Федерального закона от 29 ноября 2010 года №326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» и Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации».

4. Структура и состав защищённой сети

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

4.2. Центр управления Защищённой сетью расположен в Государственном бюджетном учреждении здравоохранения «Медицинский информационно – аналитический центр Калининградской области» (далее – МИАЦ).

4.3. Программное обеспечение и программно–аппаратные комплексы, обеспечивающие функционирование Защищённой сети:

– ViPNet [Администратор];

– Программное обеспечение ViPNet [Координатор];

– Программно-аппаратный комплекс ViPNet [Координатор];

– ViPNet [Клиент].

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

4.4.1. Серверы ViPNet [Координатор].

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

– шифрование трафика между Участниками и ЦОД;

– 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 [Координаторов] Защищенной сети определяется Центром управления Защищённой сетью и базируется на формируемых им справочниках и маршрутных таблицах.

4.4.2. 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 к информационным системам.

4.5. Режим работы Защищённой сети.

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

5. Категории пользователей защищённой сети

5.1. Администратор Защищённой сети.

5.1.1. Пользователь данной категории осуществляет администрирование Защищённой сети.

5.1.2. Функции и полномочия Администратора Защищенной сети определяются в разделе 7 настоящего Регламента.

5.2. Локальный администратор Защищённой сети.

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

5.2.2. Функции и полномочия Локального администратора определяются в разделе 8 настоящего Регламента.

5.3. Абонент Защищённой сети.

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

5.3.2. Функции и полномочия Абонента Защищенной сети (далее – Абонент) определяются пунктом 9 настоящего Регламента, а также его служебными обязанностями.

6. Сервисы защищённой сети

6.1. Абоненты получают доступ к информационным системам и ресурсам Защищённой сети.

6.2. Защищённый доступ к информационным системам.

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

6.2.2. Основными функциями защищённого доступа к информационным системам являются:

– защита трафика, передаваемого по выделенным и открытым каналам при обращении к серверам баз данных;

– разграничение доступа к информационным системам.

7. Функции и полномочия Администратора Защищенной сети

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

7.2. Обязанности Администратора Защищенной сети:

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

– ежемесячное формирование в электронном виде реестра Участников и информационных систем, подключенных к Защищённой сети;

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

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

– проведение мероприятий по модернизации и развитию Защищённой сети;

– предоставление Участникам, по заявкам их руководителей, доступа к информационным системам Защищённой сети;

– 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;

– периодические проверки с использованием сертифицированных ФСТЭК России средств защиты информации (сканеры угроз, системы обнаружения вторжений) наличия незащищенного трафика;

– информирование Локальных администраторов о порядке работы и ответственности за нарушение настоящего Регламента, а также о выявленных нарушениях;

– информирование Локальных администраторов о проводимых работах по обслуживанию и возможных перебоях в работе Защищённой сети.

7.3. Права Администратора Защищенной сети.

Для выполнения своих обязанностей Администратор Защищенной сети имеет право:

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

– вносить предложения по привлечению для технического обслуживания и администрирования оборудования Защищённой сети сторонние организации на договорной основе.

– производить отключение или ограничение доступа, по решению руководства МИАЦ, к информационным системам Защищённой сети в случаях нарушения сотрудниками Участника требований настоящего Положения и Регламента.

7.4. Ответственность Администратора Защищенной сети.

Администратор Защищенной сети несёт ответственность за:

– невыполнение требований настоящего Регламента, 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.

8. Функции и полномочия локального администратора

8.1. Локальный администратор осуществляет администрирование информационных систем и абонентских пунктов защищённой сети, 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.

8.2. Обязанности Локального администратора:

– Организация работ по подключению Абонентских пунктов и информационных систем к Защищённой сети;

– формирование учётных записей для организации доступа к информационным системам;

– информирование Абонентов о порядке работы в Защищённой сети и ответственности за нарушение данного Регламента на объектах информатизации Участника;

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

– уведомление руководителя Участника и Администратора Защищенной сети о случаях нарушений и принятых мерах;

– ознакомление Абонентов с правилами работы и требованиями безопасности Защищённой сети;

– обеспечение бесперебойного функционирования Абонентских пунктов;

– ведение организационно-распорядительной и технической документации по работе в Защищенной сети.

8.3. Права Локального администратора.

Для выполнения своих обязанностей Локальный администратор имеет право:

– сообщать непосредственному руководителю и Администратору Защищенной сети о действиях Абонентов, осуществивших несанкционированный доступ к ресурсам Защищённой сети или нарушивших другие требования по обеспечению безопасности информации и бесперебойной работе Защищённой сети;

– обращаться к Администратору Защищенной сети для решения вопросов по предоставлению доступа Участникам к Защищенной сети;

– предоставлять Администратору Защищенной сети предложения, касающиеся разработки единых правил формирования, развития и работы Защищённой сети.

8.4. Ответственность Локального администратора.

Локальный администратор несёт ответственность за:

– невыполнение требований настоящего Регламента, 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.

9. Общие правила работы Абонентов

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

9.2. Абонент обязан:

– знать правила нормативно правовых и локальных актов в сфере обеспечения информационной безопасности в Защищённой сети;

– при работе в Защищённой сети выполнять только служебные задания;

– при появлении информационных сообщений средств защиты информации о появлении вредоносных программ 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.

9.3. 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.

9.4. 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.

9.5. Ответственность Абонента.

Абонент несёт ответственность за:

– невыполнение требований настоящего Регламента, 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.

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

10. Технические мероприятия

10.1. Технические мероприятия по обслуживанию компонентов Защищенной сети и информационных систем проводятся Администратором Защищенной сети, при необходимости с привлечением Локального администратора соответствующего Участника, а также с привлечением специализированной организации на договорной основе.

10.2. В случае возникновения производственной необходимости проведения аварийных и планово-профилактических работ, доступ в Защищённую сеть может быть ограничен.

10.3. Плановые работы проводятся по графику, разрабатываемому Администратором Защищенной сети.

10.4. К плановым работам относятся:

– обновление программно-аппаратных и программных ViPNet [Координаторов];

– изменение прав доступа Абонентам;

– изменение состава программного и/или аппаратного комплексов Защищённой сети в МИАЦ;

– техническое обслуживание компонентов Защищённой сети;

– другие виды работ, необходимость которых определяется Администратором Защищенной сети.

10.5. О проведение плановых работ Администратор Защищенной сети уведомляет Локальных администраторов Участников Защищённой сети не менее чем за 24 часа до намеченного срока начала работ.

10.6. Функционирование Защищенной сети в аварийном режиме.

Для защиты компонентов Защищённой сети от сбоев электропитания серверы ViPNet [Координатор], серверы баз данных оборудуются источниками бесперебойного питания, мощность которых в случае отключения электропитания обеспечивает возможность корректного завершения выполняемых задач.

10.7. В случае возможных нештатных ситуаций Локальные администраторы, при необходимости с привлечением Администратора Защищенной сети, восстанавливают работоспособность компонентов Защищённой сети в технологически возможный короткий срок, а также для восстановления работоспособности защищённой сети или её компонентов возможно привлечение специализированной организации на договорной основе.

11. Порядок организации подключения участников к Защищенной сети

11.1. Организация подключения Участников к Защищённой сети включает в себя следующие стадии:

– выполнение требований к организации рабочего места Участником;

– подготовка и подача Администратору Защищенной сети заявки на подключение в соответствии с приложением к настоящему Регламенту;

– рассмотрение заявки Администратором Защищенной сети;

– закупка программного обеспечения или программно-аппаратных комплексов для организации защищенного доступа к ЦОД;

– формирование и передача ключевой информации;

– формирование и передача учётных записей для доступа к информационным системам.

11.2. Выполнение требований к организации рабочего места Участником.

Перед организацией подключения Претендент обязан оборудовать Абонентский пункт АРМ или технической станцией согласно техническим требованиям, предъявляемым в Приложении №1, а также выполнить требования, предъявляемые к обеспечению информационной безопасности АРМ, подключаемого к Защищенной сети.

11.3. Подготовка и подача Администратору Защищенной сети заявки на подключение в соответствии с приложением к настоящему Регламенту.

Участник, инициирующий подключение к Защищённой сети (далее – Претендент) направляет в адрес МИАЦ в отсканированном виде заявку о необходимости подключиться к Защищённой сети (Приложение №2). Заявления направляются на следующий электронный адрес:

miac@infomed39.ru;

11.4. Рассмотрение заявки Администратором Защищенной сети.

МИАЦ в течение 2-х рабочих дней со дня получения заявления о намерении подключиться к Защищённой сети, проводит оценку оснований для подключения Претендента к Защищённой сети, технической возможности организации направлений связи и доступа к информационным системам.

Приобретение программного обеспечения ViPNet [Клиент] или ViPNet [Координатор], до рассмотрения заявления о намерении подключиться к Защищённой сети, не является основанием и гарантией подключения Претендента к Защищённой сети.

Решение о подключении Претендента к Защищённой сети, направляется в виде отсканированного документа в адрес Претендента в течение 2-х рабочих дней со дня принятия указанного решения.

МИАЦ имеет право отказать Претенденту в подключении к Защищённой сети с указанием причин мотивированного отказа. Решение об отказе в подключении Претендента к Защищённой сети направляется в виде отсканированного документа в адрес Претендента.

11.5. Закупка программного обеспечения ViPNet [Клиент] или ViPNet [Координатор] Претендентом.

11.5.1. В случае принятия положительного решения о подключении к Защищённой сети, Претендент самостоятельно приобретает программное обеспечение ViPNet [Клиент] или ViPNet [Координатор] или программно-аппаратный комплекс ViPNet [Координатор].

11.5.2. При оформлении договорных отношений по приобретению программного обеспечения ViPNet [Клиент] или ViPNet [Координатор], или программно-аппаратного комплекса ViPNet [Координатор], Претендент указывает номер Защищённой сети для подключения – 763.

11.5.3. Подключение Претендента к Защищённой сети осуществляется МИАЦ, только после получения регистрационных файлов от производителя программного обеспечения или представителя производителя программного обеспечения.

11.5.4. МИАЦ уведомляет Претендента о получении регистрационных файлов.

11.6. Формирование и передача ключевой информации.

11.6.1. Формирование и передача ключевой информации осуществляются в течение 3-х рабочих дней со дня получения регистрационных файлов на подключение, при этом МИАЦ:

– производит регистрацию Абонентских пунктов и Абонентов в Центре управления сетью;

– организует настройку узлов между Абонентскими пунктами и ЦОД, в соответствии с заявкой на подключение;

– формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему;

– по завершению работ уведомляет об этом Претендента.

11.6.2. Претендент для получения дистрибутива ключей и пароля доступа к нему должен:

а) Предоставить в адрес МИАЦ:

– копии приказов о назначении Локального администратора;

– копии соглашений с Локальным администратором о неразглашении информации, к которой будет получен доступ в связи с выполнением своих функций (Приложение №3);

б) Направить в МИАЦ Локального администратора с доверенностью на получение дистрибутива ключей (Приложение №4).

Факт выдачи дистрибутива ключей, заносится в Журнал учёта выдачи ключевых документов (Приложение №5).

12. Организация межсетевого взаимодействия с другими сетями ViPNet

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

– подготовка и подача Администратору Защищенной сети заявки на подключение в соответствии с приложением к настоящему Регламенту;

– рассмотрение заявки Администратором Защищенной сети;

– формирование и передача ключевой информации.

12.2. Подготовка и подача Администратору Защищенной сети заявки на подключение в соответствии с приложением к настоящему Регламенту.

Для организации межсетевого взаимодействия между Защищённой сетью и защищенной ViPNet сетью Претендента Локальный администратор готовит заявление, в котором уведомляет МИАЦ о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц ответственных за организацию межсетевого взаимодействия.

12.3. Рассмотрение заявки Администратором Защищенной сети.

12.3.1. В случае получения информационного письма МИАЦ в течение 2-х рабочих дней со дня его получения проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

12.3.2. МИАЦ имеет право отказать в организации межсетевого взаимодействия, указав причину мотивированного отказа.

12.3.3. В случае принятия решения об организации межсетевого взаимодействия, МИАЦ в течение 2-х рабочих дней в виде отсканированного документа уведомляет о принятии такого решения Претендента.

12.4. Формирование и передача ключевой информации

12.4.1. В случае принятия решения об организации межсетевого взаимодействия, Локальный администратор, в соответствии с актуальным «Руководством администратора» на ViPNet [Администратор], производит формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой их сетей и доверенным способом передает сформированный экспорт Администратору Защищенной сети.

12.4.2. После завершения процедуры организации межсетевого взаимодействия между Защищенной сетью и Защищенной сетью ViPNet Претендента подписывается Протокол установления межсетевого взаимодействия (Приложение №6).

13. Ответственность

13.1. МИАЦ несет ответственность за:

– администрирование Защищенной сети в части организации связей между Абонентами и ЦОД;

– своевременное выполнение мероприятий, указанных в настоящем Регламенте.

13.2. МИАЦ не несет ответственность за:

– установку и настройку абонентских пунктов Участника.

13.3. Участник несет ответственность за:

– выполнение требований, предъявляемых к обеспечению безопасности Защищенной сети (Приложение № 1);

– установку и настройку Абонентского пункта Участника;

– своевременную актуализацию передаваемых в МИАЦ документов в соответствии с настоящим Регламентом.

14. Компрометация ключей

14.1. К событиям компрометации, когда ключи Абонента считаются скомпрометированными, относятся следующие случаи:

– посторонним лицам мог стать доступен (стал доступен) файл ключевого дистрибутива Абонента;

– посторонним лицам мог стать доступен (стал доступен) съёмный носитель ключевой информации Абонента;

– посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте;

– прекращение полномочий Абонента или Локального администратора, согласно соответствующему приказу, имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора (договора возмездного оказания услуг).

14.2. При угрозе доступа посторонних лиц к ключевой информации доступа Абонента, в том числе компрометации, при старте модуля ViPNet Client, при условии, что доступ к Абонентскому пункту посторонних лиц был невозможен, Локальному администратору следует сменить пароль и разрешить Абонентам продолжить работу.

14.3. При угрозе доступа посторонних лиц к ключевой информации доступа Абонента, в том числе компрометации, при старте модуля ViPNet Client, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, наступает:

– прекращение полномочий Абонента;

– прекращение полномочий Локального администратора ключевая информация всех Абонентов Участника считается скомпрометированной.

14.4. В случае наступления любого из событий, связанных с компрометацией ключевой информации, Абонент немедленно прекращает связь с другими Абонентскими пунктами и сообщает о факте компрометации своему Локальному администратору.

14.5. Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Администратора Защищенной сети.

14.6. Администратор Защищенной сети при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

– в программном обеспечении ViPNet [Администратор] объявить ключи Абонентского пункта скомпрометированными и создать средствами программного обеспечения справочники связей при компрометации с необходимой информацией;

– оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом, ключевая информация которого была скомпрометирована;

– сформировать средствами программного обеспечения ViPNet [Администратор] новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи.

Приложение № 1
к Регламенту

Технические требования по подключению пользователей к защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области»

1. Технические требования к характеристикам автоматизированных рабочих мест

1.1. Для подключения к информационным ресурсам «Единой государственной информационной системы в сфере здравоохранения Калининградской области» (далее – ЕГИСЗ) Участник должен иметь автоматизированное рабочее место, удовлетворяющее следующим требованиям:

1.1.1. Аппаратное обеспечение:

– процессор с производительностью не ниже 1700 МГц;

– объем оперативной памяти не менее 1 ГБ.

1.1.2. Программное обеспечение:

– операционная система: актуальной версии получающей обновления безопасности - GNU Linux/MacOS/Windows (редакции «профессиональная»);

– интернет-браузер: Mozilla Firefox (последней версии).

1.1.3. Наличие доступа в сеть Интернет или наличие подключения объекта информатизации к ЕГИСЗ по выделенным волоконно-оптическим каналам передачи данных IP MPLS (в случае подключения диагностического и лабораторного оборудования).

2. Организация защищенного канала связи

2.1. Для построения защищенного канала связи с использованием криптографических методов защиты Претендент на подключение к Защищенной сети обязан использовать «ViPNet Client» или «ViPNet Coordinator»:

– программное обеспечение «ViPNet Client (КС2)» сертифицированной версии на каждом подключаемом АРМ, если количество АРМ, подключаемых к ЕГИСЗ не более 5 включительно;

– программно-аппаратный комплекс «ViPNet Coordinator HW 100», если количество АРМ, подключаемых к ЕГИСЗ от 6 до 50 включительно;

– программно-аппаратный комплекс «ViPNet Coordinator HW 1000», если количество АРМ, подключаемых к ЕГИСЗ превышает 50.

Установка программного обеспечения «ViPNet Coordinator» не допускается в связи с прекращением действия сертификата соответствия ФСБ России.

3. Требования к составу организационных и технических мер по обеспечению безопасности информации

3.1. Для осуществления подключения к информационным ресурсам ЕГИСЗ на АРМ должны быть выполнены мероприятия, связанные с выполнением требований по обеспечению безопасности информации.

3.2. На АРМ должны быть установлены и настроены в соответствии с требованиями эксплуатационной документации средства защиты информации, сертифицированные ФСТЭК и обеспечивающие:

– доверенную загрузку (исполнение в формате платы расширения);

– антивирусную защиту;

– защиту от несанкционированного доступа;

– контроль съемных носителей;

– обнаружение вторжений, для АРМ подключенных через сеть Интернет.

3.3. Для доступа к операционной системе АРМ должна обеспечиваться усиленная аутентификация и идентификация пользователя по индивидуальному идентификатору, размещенному на носителе, сертифицированным ФСТЭК России.

3.4. У Участника должен быть разработан комплект организационно-распорядительной и технической документации, регламентирующей обеспечение информационной безопасности, в соответствии с требованиями Администратора Защищенной сети.

Приложение № 2
к Регламенту

Директору МИАЦ
_____
_____

ЗАЯВЛЕНИЕ

На подключение к защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области»

Наименование организации	
Адрес месторасположения узлов	
ИНН/ОГРН	
Наименование подключаемой информационной системы	
Цель подключения	
Предполагаемое число подключаемых узлов	
ФИО, должность ответственного за подключение (Локального администратора)	
Контактный телефон ответственного за подключение	
Адрес электронной почты ответственного за подключение	

Прошу подключить к защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области» с помощью *приобретения программного обеспечения ViPNet [Клиент] / ViPNet [Координатор]/ организации межсетевого взаимодействия с сетью ____ (сеть претендента)* в соответствии с вышеуказанной информацией и на условиях согласно Регламенту защищённой виртуальной сети ViPNet Государственного бюджетного учреждения здравоохранения «Медицинский информационно – аналитический центр Калининградской области». Настоящим подтверждаем выполнение всех требований по обеспечению информационной безопасности для подключения к Защищенной сети. Уведомлены об ответственности за несоблюдение требований законодательства в сфере защиты информации.

Руководитель организации:

Должность:_____
ФИО:_____
Подпись:_____
«____»_____20___г.

М. П.

Приложение №3
к Регламенту

ОБЯЗАТЕЛЬСТВО
о неразглашении сведений конфиденциального характера

Я, _____
_____
(Ф.И.О., должность)

обязуюсь:

а) не разглашать сведений, составляющих конфиденциальную информацию, которые мне будут доверены или станут известны при выполнении должностных обязанностей;

б) выполнять относящиеся ко мне требования приказов, инструкций и положений по защите информации, с которыми я ознакомлен (а);

в) в случае попытки посторонних лиц получить от меня информацию конфиденциального характера, немедленно сообщать об этом своему непосредственному начальнику;

г) в случае увольнения, не разглашать и не использовать для себя или других сведения, составляющие конфиденциальную информацию.

В случае увольнения с работы, я обязуюсь неукоснительно соблюдать требования пункта «а» настоящего обязательства.

Я предупрежден (а), что за разглашение сведений, составляющих конфиденциальную информацию, или утрату документов и предметов, содержащих такие сведения, а также иные нарушения режима безопасности информации, буду привлечен (а) к административной или иной ответственности в соответствии с действующим законодательством РФ.

«____» _____ 20____ г. _____
(подпись)

Приложение №4
к Регламенту

(Выполняется на бланке Участника)

Доверенность

на получение дистрибутива ключей

_____ в лице
(наименование Участника)

_____,
(Руководитель)

действующего на основании _____, уполномочивает:

_____, паспорт_____,
(ФИО) *(серия, номер)*

выданный

_____,
(когда и кем, включая код подразделения)

получить в Государственном бюджетном учреждении здравоохранения «Медицинский информационно–аналитический центр Калининградской области» дистрибутив ключей для первичного запуска прикладной программы сети ViPNet.

Настоящая доверенность действительна по «___» _____ 20___г.

Подпись лица, получившего доверенность _____

_____	_____	_____
(Должность руководителя Участника)	*(Подпись)*	*(ФИО руководителя Участника)*

Приложение №5
к Регламенту

ЖУРНАЛ УЧЁТА ВЫДАЧИ КЛЮЧЕВЫХ ДОКУМЕНТОВ

12	Дата выдачи	Организация	Ф.И.О. пользователя	Идентификатор дистрибутива	Тип носителя	Способ передачи	Подпись получившего (отправившего по ДП)	Отметка об уничтожении

Приложение №6
к Регламенту

ПРОТОКОЛ
установления межсетевого взаимодействия

«____» _____ 20__г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организаций

2. Целью установление межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet сетей указанных организаций.
3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№_____		
№_____		

4. Передача начального и ответного экспорта между сетями №___ и №___

осуществлялась через специалиста, уполномоченного на данные действия.

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

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

в сети №___ - «_____»
в сети №___ - «_____»

7. Смена межсетевых ключей, изменение состава Абонентских пунктов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чём администраторы защищённых сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] с указанием производимых изменений.

8. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищённых сетей, которые могут привести к нарушению межсетевого взаимодействия.

Администратор сети ViPNet №_____ _____ _____ (ФИО) _____ (подпись) «___»_____20___г. М.П.	Администратор сети ViPNet №_____ _____ _____ (ФИО) _____ (подпись) «___»_____20___г. М.П.

Приложение №7
к Регламенту

Директору МИАЦ
ул. Клиническая, 74, г. Калининград, 236016

_____

от _____

_____
(Ф.И.О.)

паспорт серия_____№ _____

выдан _____

_____
(кем, число, месяц и год, код подразделения)

Заявление

Я, _____,
(фамилия, имя и отчество полностью)

даю свое согласие на сбор систематизацию, накопление, хранение, уточнение (обновление и изменение), использование, распространение (передачу), обезличивание, блокировку и уничтожение своих персональных данных содержащихся в копии основного документа, удостоверяющего личность в целях доступа к Региональному сегменту единой государственной информационной системы в сфере здравоохранения Калининградской области.

Настоящее согласие действует со дня его подписания до дня предоставления соответствующего отзыва в письменной форме.

«___» _____ 20__ г. _____ /_____/