ДЕПАРТАМЕНТ ЗДРАВООХРАНЕНИЯ ОРЛОВСКОЙ ОБЛАСТИ

П Р И К А З

26 февраля 2019г. № 101

г. Орёл

Об утверждении регламента организации подключения к защищенной виртуальной сети ViPNet №1322

В целях организации безопасности сети сети ViPNet №1322 Департамента здравоохранения Орловской области, приказываю:

1. Утвердить «Регламент организации подключения к защищенной виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области» (Приложение 1).
2. БУЗ Орловской области «МИАЦ» довести Регламент до сведения всех абонентов защищенной виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области.
3. Контроль за исполнением приказа возложить на заместителя руководителя Департамента – начальника управления здравоохранения Орловской области П. В. Сергеева.

Член Правительства Орловской области – руководитель Департамента здравоохранения Орловской области И. А. Залогин

Приложение 1

УТВЕРЖДАЮ

член Правительства Орловской области

– руководитель Департамента

здравоохранения Орловской области

_____ И.А. Залогин

«____» февраля 2019г.

РЕГЛАМЕНТ
ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ К ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET №1322 ДЕПАРТАМЕНТА ЗДРАВООХРАНЕНИЯ ОРЛОВСКОЙ ОБЛАСТИ

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящей Политике используются следующие понятия:

Абонент – сотрудник Участника, на рабочем месте которого установлено программное обеспечение ViPNet [Клиент].

Абонентский пункт – персональный компьютер с установленным программным обеспечением ViPNet [Клиент].

Администратор – назначенный приказом сотрудник Участника, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному Участнику.

Главный администратор – сотрудник Оператора, осуществляющий общую политику администрирования всей Защищенной сети.

Защищенная сеть – защищенная виртуальная сеть Департамента здравоохранения Орловской области, построенная по технологии ViPNet.

Компрометация ключей – факт доступа постороннего лица к защищаемой информации, а также подозрение на данный факт.

Координатор Защищённой сети – назначенный приказом директора сотрудник бюджетного учреждения здравоохранения Орловской области «Медицинский информационно-аналитический центр», определяющий общую стратегию развития Защищённой сети.

Локальный администратор – назначенный приказом сотрудник Участника системы здравоохранения, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному участнику.

Оператор – бюджетное учреждение здравоохранения Орловской области «Медицинский информационно-аналитический центр».

Обслуживающая организация – организация, выполняющая администрирование сети ViPNet №1322 и имеющая лицензии ФСБ России (на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации) и

ФСТЭК России (на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, установки, монтажа, средств защиты информации).

Претендент – организация, имеющая намерения подключиться к Защищенной сети.

СКЗИ – средства криптографической защиты информации**.**

Участник – организация, подключенная к Защищенной сети в установленном в настоящем регламенте порядке.

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

ViPNet [Администратор] – программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой сетью ViPNet.

ViPNet [Клиент] – программное обеспечение, реализующее на рабочем месте или сервере функцию VPN-клиента, межсетевого экрана и клиента защищённой почтовой службы.

ViPNet [Координатор] – программное или программно-аппаратное обеспечение, выполняющее функции универсального сервера виртуальной защищённой сети ViPNet.

VPN (Virtual Private Network) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1 Регламент взаимодействия участников защищенной сети ViPNet Департамента здравоохранения Орловской 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»;

– Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи».

2.2. Регламент определяет и устанавливает:

– порядок организации и подключения Участников Защищенной сети (далее – Участники) к защищённой виртуальной сети ViPNet Департамента здравоохранения Орловской (далее – Защищённая сеть);

– порядок предоставления доступа к информационным системам Защищённой сети;

– порядок организации защищённого межсетевого взаимодействия;

– порядок разрешения конфликтных ситуаций.

2.3 Нарушение положений настоящего Регламента может являться основанием отключения Участника от Защищенной сети.

3. ПОРЯДОК ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ УЧАСТНИКОВ К ЗАЩИЩЁННОЙ СЕТИ

3.1 Организация подключения Участников к Защищенной сети включает в себя следующие стадии:

– заявительная стадия;

– стадия рассмотрения заявления;

– Закупка программного обеспечения ViPNet [Клиент] Претендентом;

– формирование и передача ключевой информации;

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

3.2 Заявительная стадия.

Участник, желающий подключиться к Защищенной сети (далее – Претендент) направляет в адрес БУЗ Орловской области «МИАЦ» заявление о намерении подключиться к Защищенной сети (Приложение №1).

3.2.1 В заявлении должна содержаться следующая информация:

– предполагаемое количество подключаемых Абонентских пунктов;

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

– перечень информационных систем, к которым необходимо организовать доступ;

– ФИО и контактный телефон лица, ответственного за подключение Претендента.

3.3 Стадия рассмотрения заявления.

3.3.1 БУЗ Орловской области «МИАЦ» после получения заявления о намерении подключиться к Защищенной сети, проводит оценку оснований для подключения Претендента к Защищенной сети, технической возможности организации направлений связи и доступа к информационным системам, при необходимости изменяет перечень обязательных мер и средства защиты обрабатываемой информации применяемых Претендентом.

3.3.2 Приобретение программного обеспечения ViPNet [Клиент] до рассмотрения заявления о намерении подключиться к Защищенной сети не является основанием и гарантией подключения Претендента к Защищенной сети.

3.3.3 Решение о подключении Претендента к Защищенной сети направляется в письменной форме в адрес Претендента.

3.3.4 БУЗ Орловской области «МИАЦ» имеет право отказать Претенденту в подключении к Защищенной сети, объяснив причину отказа.

Решение об отказе в подключении Претендента к Защищенной сети направляется в письменной форме в адрес Претендента.

3.3.5 БУЗ Орловской области «МИАЦ» уведомляет Претендента о принятии решения о подключении (отказе в подключении) к Защищенной сети посредством электронной почты, указанной в заявление о намерении подключиться к Защищенной сети, со ссылкой на соответствующее решение.

3.4 Закупка программного обеспечения ViPNet [Клиент] Претендентом.

3.4.1 В случае принятия положительного решения о подключении к Защищенной сети Претендент обращается в Обслуживающую организацию или стороннюю организацию, имеющую лицензии ФСБ России (на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации) и ФСТЭК России (на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, установки, монтажа средств защиты информации), для приобретения и установки программного обеспечения ViPNet [Клиент], средства защиты от несанкционированного доступа и антивирусного средства, сертифицированных по требованиям безопасности ФСТЭК России.

3.4.2 При оформлении договорных отношений по приобретению программного обеспечения ViPNet [Клиент] Претендент указывает номер Защищенной сети для подключения – 1322.

3.4.3 Подключение Претендента к Защищенной сети осуществляется Обслуживающей организацией только после получения регистрационных файлов от производителя программного обеспечения или представителя производителя программного обеспечения.

3.4.4 Обслуживающая организация уведомляет Претендента о получении регистрационных файлов.

3.5 Формирование и передача ключевой информации.

3.5.1 Претендент после получения информации о поступлении регистрационных файлов формирует и направляет в БУЗ Орловской области «МИАЦ» заявку на подключение (Приложение №2).

3.5.2. С момента получения от БУЗ Орловской области «МИАЦ» копии заявки на подключение Обслуживающая организация:

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

– организовывает направления связи между Абонентскими пунктами в соответствии с заявкой на подключение;

– формирует дистрибутивы ключей для Абонентских пунктов;

– по завершении обозначенных работ уведомляет об этом Претендента.

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

а) Предоставить в адрес БУЗ Орловской области «МИАЦ»:

– копию приказа о назначении Локального администратора (Приложение №3) и Абонентов Защищённой сети (Приложение №4);

– копии соглашений с Локальным администратором и Абонентами Защищённой сети о неразглашении информации, к которой будет получен доступ в связи с выполнением своих функций (Приложение №5);

– копию акта установки и настройки средств защиты информации от несанкционированного доступа и антивирусной защиты;

б) Направить администратора в Обслуживающую организацию с доверенностью на получение дистрибутива ключей (Приложение №6).

3.5.4 Факт выдачи дистрибутива ключей заносится Обслуживающей организацией в Журнал учёта выдачи ключевых документов (Приложение №7).

3.5.5 Претендент для получения доступа к информационным системам Участников должен предоставить в адрес БУЗ Орловской области «МИАЦ» копию документа, подтверждающего согласие Владельца информационной системы (далее – Владельца) на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является БУЗ Орловской области «МИАЦ», выполнение пункта 3.5.5 не требуется).

4. ПОРЯДОК ИЗМЕНЕНИЯ НАПРАВЛЕНИЙ СВЯЗИ И/ИЛИ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

4.1 Порядок изменения направлений связи и/или предоставление доступа к информационным системам включает в себя следующие стадии:

– заявительная стадия;

– стадия рассмотрения заявки;

– формирование и передача ключевой информации;

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

4.2 Заявительная стадия.

4.2.1 Участник, желающий изменить направление связей и/или получить доступ к информационным системам Защищенной сети, направляет в адрес БУЗ Орловской области «МИАЦ» заявку за подписью руководителя (Приложение №8) и копию документа, подтверждающего согласие Владельца на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является БУЗ Орловской области «МИАЦ», выполнение пункта 4.2.1 не требуется).

4.2.2 При заполнении заявки следует указывать все необходимые на данный момент направления связи и все информационные системы Защищенной сети, к которым необходим доступ.

4.3 Стадия рассмотрения заявки.

4.3.1 БУЗ Орловской области «МИАЦ» после получения рассматривает заявку, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным системам Защищенной сети.

4.3.2 Решение об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети направляется в письменной форме в адрес Участника.

4.3.3 БУЗ Орловской области «МИАЦ» имеет право отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, объяснив причину отказа. Решение об отказе в изменении направлений связи и/или организации доступа к информационным системам Защищенной сети направляется в письменной форме в адрес Претендента.

4.3.4 БУЗ Орловской области «МИАЦ» уведомляет Претендента об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети, посредством электронной почты, со ссылкой на соответствующее Решение.

4.3.5 Формирование и передача ключевой информации.

4.3.6 С момента уведомления Участника о принятии решения об изменении направлений связи и/или организации доступа к информационным системам Защищенной сети Обслуживающая организация:

– вносит изменения в направления связей между Абонентскими пунктами в соответствии с заявлением;

– формирует необходимую справочную и ключевую информацию;

– через Центр управления сетью направляет справочную и ключевую информацию на соответствующие Абонентские пункты Участника;

– по завершении обозначенных работ уведомляет об этом Участника.

4.3.7 При поступлении на Абонентский пункт новая ключевая информация автоматически обновляет существующую ключевую информацию.

4.3.8 Формирование и передача учётных записей для доступа к информационным системам.

4.3.9 Локальный администратор Владельца формирует учётные записи для доступа к информационным системам и передаёт их Локальному администратору Участника в сроки и на согласованных ранее условиях.

5. ОРГАНИЗАЦИЯ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ С ДРУГИМИ СЕТЯМИ VIPNET

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

– заявительная стадия;

– рассмотрение заявления;

– формирование и передача ключевой информации;

5.2 Заявительная стадия.

5.2.1 Для организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet Координатор Защищённой сети или администратор сторонней сети ViPNet готовят информационное письмо, в котором информируют другую сторону о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц, ответственных за организацию межсетевого взаимодействия.

5.3 Рассмотрение заявления.

5.3.1 БУЗ Орловской области «МИАЦ» после получения информационного письма проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

5.3.2 БУЗ Орловской области «МИАЦ» имеет право отказать в организации межсетевого взаимодействия, объяснив причину отказа.

5.3.3 В случае принятия решения об организации межсетевого взаимодействия БУЗ Орловской области «МИАЦ» и Участник межсетевого взаимодействия разрабатывают и подписывают соглашение об информационном взаимодействии.

5.4 Формирование и передача ключевой информации.

5.4.1 В случае принятия решения об организации межсетевого взаимодействия Обслуживающая организация и администратор сторонней сети ViPNet, в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]», производят формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой сети.

5.4.2 Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие Центры управления сетей (далее – ЦУС), с которыми должно осуществляться межсетевое взаимодействие.

5.4.3 Во всех ЦУС в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]» производится ввод и обработка (импорт) полученных из других ЦУС данных (начального экспорта), установление связей своих Абонентских пунктов с Абонентскими пунктами ЦУС, предоставившими информацию (ответный экспорт) для ЦУС, приславших первичную информацию, включая свои сертификаты.

5.4.4 Ответная информация (ответный экспорт) доверенным способом передается в соответствующие ЦУС, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого взаимодействия между ЦУС, в дальнейшем обмен данными между ними производится в автоматическом режиме.

5.4.5 Сформированная ключевая и справочная информация через ЦУС отправляется на Абонентские пункты, участвующие в межсетевом взаимодействии.

5.4.6 После завершения процедуры организации межсетевого взаимодействия между Защищённой сетью и сторонней сетью ViPNet

подписывается Протокол установления межсетевого взаимодействия (Приложение №9).

5.5 Организация направлений связи между Абонентскими пунктами Участников и Абонентскими пунктами сторонней сети ViPNet, с которой установлено межсетевое взаимодействие, осуществляется в соответствии с разделом 4 настоящего Регламента.

6. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ ПЛАНОВОЙ СМЕНЫ МЕЖСЕТЕВОГО МАСТЕР-КЛЮЧА.

6.1 Порядок модификации межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа предполагает выполнение ряда технологических и организационных мероприятий.

6.2 Предварительные организационные мероприятия.

Перед тем как осуществлять плановую смену межсетевого мастер-ключа, Обслуживающая организация и администратор сторонней сети ViPNet, с которой установлено межсетевое взаимодействие должны:

– выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;

– в случае использования симметричного мастер-ключа выбирается сеть, в которой будет создан новый межсетевой мастер-ключ;

– выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для Абонентских пунктов сетей.

6.3 Формирование нового межсетевого мастер-ключа.

Формирование нового межсетевого мастер-ключа производится в соответствии с «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]».

6.4 Процедура создания экспорта и приёма импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приём импортированных данных в

соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]».

6.5 Межсетевое взаимодействие после смены межсетевого мастер-ключа.

После смены межсетевого мастер-ключа связь между взаимодействующими Абонентскими пунктами Защищённой сети и ViPNet сети, с которой установлено межсетевое взаимодействие, возможна только после прохождения обновления ключевой информации на всех соответствующих Абонентских пунктах.

6.6 Обновленная ключевая информация через ЦУС отправляется на Абонентские пункты, участвующие в межсетевом взаимодействии.

7. КОМПРОМЕТАЦИЯ КЛЮЧЕЙ

7.1 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;

– на Абонентском пункте отсутствовал (был отключен) модуль ViPNet Client Monitor и в локальной сети считается возможным присутствие посторонних лиц;

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

7.2 При возникновении сомнений в неизвестности посторонним лицам пароля доступа Абонента при старте модуля ViPNet Client Monitor, при

условии, что доступ к Абонентскому пункту посторонних лиц был невозможен, Локальному администратору следует сменить пароль и разрешить Абонентам продолжить работу.

7.3 При возникновении сомнений в неизвестности посторонним лицам пароля доступа Абонента при старте модуля ViPNet Client Monitor, при условии, что доступ к Абонентскому пункту посторонних лиц был возможен, ключи считаются скомпрометированными.

7.4 К событиям, требующим проведения расследования и принятия решения на предмет компрометации ключевой информации, относится возникновение подозрений в утечке информации при её передаче посредством защищённой сети.

7.5 В случае прекращения полномочий Абонента, ключи данного Абонента считаются скомпрометированными.

7.6 В случае прекращения полномочий Локального администратора, ключевая информация всех Абонентов Участника считается скомпрометированной.

7.7 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.

7.8 Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Обслуживающей организации.

7.9 Обслуживающая организация при получении сообщения о компрометации ключевой информации должна:

– 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;

– произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищённой сети.

8. ПОРЯДОК ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕЙ

8.1 Компрометация ключей Абонента.

При наступлении любого из перечисленных в п. 7.1 настоящего Регламента событий Абонент должен немедленно прекратить работу на своём Абонентском пункте и сообщить о факте компрометации администратору своей сети ViPNet.

8.1.1 Администратор сети ViPNet при получении сообщения о компрометации ключевой информации 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;

– произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищённой сети.

– сформировать и отправить импорт для сети ViPNet, с Абонентскими пунктами которой взаимодействовал скомпрометированный Абонентский пункт;

8.1.2 Администратор ViPNet сети, Абоненты которой взаимодействовали с Абонентом, ключи которого скомпрометированы, после приёма и обработки импорта создаёт новую ключевую информацию своим Абонентам.

8.1.3 Возобновление межсетевого взаимодействия возможно только после прохождения обновления ключевой информации на всех взаимодействующих Абонентских пунктах.

8.2 Внеплановая смена межсетевого мастер-ключа. Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер ключа, на котором происходит организация межсетевого взаимодействия.

8.2.1 В случае компрометации симметричного межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при защищённом межсетевом взаимодействии. Межсетевое взаимодействие должно быть немедленно остановлено.

8.2.2 Для восстановления работы межсетевого взаимодействия необходимо произвести технологические и организационные мероприятия, описанные в разделе 6 «Порядок организации защищённого межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа».

8.2.3 При компрометации ключей Обслуживающая организация заносит соответствующие записи в Журнал изменений межсетевого взаимодействия.

9. НАЗНАЧЕНИЕ ОТВЕТСТВЕННЫХ ЛИЦ

9.1 Назначение Координатора.

9.1.1 Координатор назначается и отстраняется от исполнения возложенных функций приказом директора БУЗ Орловской области «МИАЦ».

9.2 Назначение Главного администратора.

9.2.1 Главный администратор назначается и отстраняется от исполнения возложенных функций приказом директора БУЗ Орловской области «МИАЦ».

9.3 Назначение Локального администратора.

9.3.1 Исполнение функций Локального администратора возлагается на сотрудника Участника.

9.3.2 Локальный администратор назначается и отстраняется от исполнения возложенных функций приказом руководителя Участника.

9.3.3 Необходимым условием назначения Локального администратора является подписание с ним соглашения о неразглашении информации, полученной вследствие выполнения своих обязанностей.

9.3.4 В случае смены сотрудника, на которого возложены функции Локального администратора, Участник обязан известить об этом Главного администратора, направив заявку (Приложение №10), и Владельца информационных систем, к которым Участник имеет доступ.

9.3.5 При заполнении заявки необходимо указывать всех назначенных на данный момент Локальных администраторов и Абонентов Участника.

9.3.6 Обслуживающая организация создаёт новые ключевые наборы для всех Абонентов Участника и передаёт их Локальному администратору.

9.3.7 Локальный администратор Владельца информационных систем, к которым Участник имеет доступ, блокирует старые и создаёт новые учётные записи всех Абонентов Участника для доступа к информационным системам в сроки и на согласованных ими условиях.

9.3.8 Копия приказа о возложении функций Локального администратора на сотрудника Участника, а также копия подписанного с этим сотрудником, соглашения о неразглашении информации полученной вследствие выполнения своих обязанностей, передаются Участником Координатору.

9.4 Назначение Абонентов.

9.4.1 Список сотрудников (Абонентов), которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, утверждается приказом руководителя Участника.

9.4.2 С каждым сотрудником (Абонентом), допущенным к работе в Защищённой сети, подписывается соглашение о неразглашении информации, полученной вследствие выполнения своих должностных обязанностей.

9.4.3 В случае изменения списка сотрудников (Абонентов), которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, Участник обязан известить об этом Координатора, направив заявку (Приложение №10), и Владельца информационных систем, к которым Участник имеет доступ.

9.4.4 При заполнении заявки необходимо указывать всех назначенных на данный момент Локальных администраторов и Абонентов Участника.

9.4.5 Обслуживающая организация создаёт новые ключевые наборы вновь назначенных Абонентов Участника и передаёт их Локальному администратору.

9.4.6 Локальный администратор Владельца информационных систем, к которым Участник имеет доступ, блокирует старые и создаёт новые учётные записи для вновь назначенных Абонентов Участника для доступа к информационным системам в сроки и на условиях, оговорённых заранее.

9.4.7 Копии приказов об утверждении списка сотрудников, которым для выполнения служебных обязанностей необходим доступ в Защищённую сеть, а также соглашения о неразглашении информации, полученной вследствие выполнения своих должностных обязанностей, подписанных с этими сотрудниками, передаются Участником Координатору.

10. ОБНОВЛЕНИЕ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, В ТОМ ЧИСЛЕ СКЗИ ЗАЩИЩЕННОЙ СЕТИ

10.1 Обновление средств защиты информации, в том числе СКЗИ Защищенной сети (ViPNet [Клиент]), производятся в случаях:

– истечения срока действия сертификата соответствия ФСТЭК России и/или ФСБ России требованиям безопасности на средства защиты информации, в том числе СКЗИ;

– возникновения технической необходимости произвести обновление средств защиты информации, в том числе СКЗИ (совместимость с новыми операционными системами, расширение функционала, увеличение производительности и т.д.).

10.2 БУЗ Орловской области «МИАЦ», при возникновении необходимости обновить средства защиты информации, в том числе СКЗИ, направляет Участникам уведомление (письмо), в котором указывается срок перехода на новые версии средств защиты информации, в том числе СКЗИ. Уведомление направляется в письменной форме в адрес Участников.

10.3 Участник, после получения уведомления, обязан обратиться в Обслуживающую организацию или стороннюю организацию, имеющую лицензии ФСБ России (на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации) и ФСТЭК России (на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищённости конфиденциальной информации от несанкционированного доступа и её модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, установки, монтажа, средств защиты информации), для приобретения и установки обновлений средств защиты информации, в том числе СКЗИ, сертифицированных по требованиям безопасности ФСТЭК России и/или ФСБ России, в срок, указанный в Уведомлении.

10.4 При оформлении договорных отношений по приобретению обновления СКЗИ (программного обеспечения ViPNet [Клиент]) Участник указывает номер Защищенной сети – 1322.

10.5 Участник уведомляет о приобретении необходимых обновлений средства защиты информации, в том числе СКЗИ, БУЗ Орловской области «МИАЦ» в письменной форме, прикладывая скан-копию страницы формуляра, в которой указаны учетные номера средств защиты информации, в том числе СКЗИ.

10.6 БУЗ Орловской области «МИАЦ» производит отключение Участника от Защищенной сети в случае невыполнения им требований п.10.3 и п.10.5 настоящего Регламента путем направления соответствующей заявки в Обслуживающую организацию.

Приложение №1
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

Директору
Бюджетного учреждения здравоохранения
Орловской области «Медицинский
информационно – аналитический центр»
Р.А. Селищеву

О подключении
к защищённой виртуальной сети
ViPNet №1322 Департамента
здравоохранения Орловской
области

Прошу подключить *Бюджетное учреждение здравоохранения Орловской области «Поликлиника №1234» г.* Орёл к защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области для обмена информацией, содержащей персональные данные, *со страховыми медицинскими организациями г. Орла, Бюджетным учреждением здравоохранения Орловской области «Медицинский информационно – аналитический центр», Территориальным фондом обязательного медицинского страхования Орловской области.*

Предполагаемое число подключаемых абонентских пунктов – *2 (два)*.

Перечень информационных систем, к которым необходим доступ: *ЕРИС «Льготное лекарственное обеспечение населения Орловской области»*.

Лицо, ответственное за подключение, и контактный телефон: *Иванов Иван Иванович, (8 486) 22-22-22, адрес электронной почты*

Руководитель организации _____ /ФИО/

М.П.

Приложение №2
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

ЗАЯВКА
на подключение к Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области

Полное наименование организации без сокращений (на основании учредительных документов)	*Бюджетное учреждение здравоохранения Орловской области «Поликлиника №1234» г. Орёл*
Сокращённое название организации	*БУЗ Орловской области «Поликлиника №1234»*
Юридический адрес организации с индексом	*г. Орёл, ул. Советская 15, 302002*
Фактический (почтовый) адрес организации с индексом	*г. Орёл, ул. Советская 15, 302002*
ФИО руководителя	*Петров Пётр Петрович*
Должность руководителя	*Главный врач*
Количество необходимых для регистрации Абонентских пунктов	*2 (два)*
Наименование Абонентских пунктов (не более 47 символов включая пробелы)	*Поликлиника №1234 – 1* *Поликлиника №1234– 2*
ФИО Абонента, зарегистрированного на Абонентском пункте	*Поликлиника №1234–1: Иванов Иван Иванович* *Поликлиника №1234 – 2: Петров Петр Петрович*
ФИО Локального администратора	*Иванов Иван Иванович*
Контактные телефоны Локального администратора	*(4862) 88-88-88*
Контактный E-mail Локального администратора	ivanov@mail.ru
Направления связи для организации защищённого обмена информацией	*- БУЗ Орловской области «Медицинский информационно – аналитический центр»;* *- ТФОМС Орловской области.*
Перечень информационных систем, к которым необходим доступ:	*ЕРИС «Льготное лекарственное обеспечение населения Орловской области»*
Наименование сертифицированного ФСТЭК России средства защиты от несанкционированного доступа	
Наименование сертифицированного ФСТЭК России антивирусного средства защиты	

_____ _____/_____

Дата ФИО / Подпись

Приложение №3
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ОРЛОВСКОЙ ОБЛАСТИ «ПОЛИКЛИНИКА №1234» Г.ОРЁЛ

П Р И К А З

«___» _____2019 г. **№____**

О назначении Локального администратора БУЗ Орловской области «Поликлиника №1234» г. Орёл.

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и Абонентских пунктов, принадлежащих БУЗ Орловской области «Поликлиника №1234» г.Орёл и относящихся к защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором БУЗ Орловской области «Поликлиника №1234» г.Орёл: Иванова Ивана Ивановича - инженера АСУ БУЗ Орловской области «Поликлиника №1234»;
2. В своей работе по выполнению функций Локального администратора БУЗ Орловской области «Поликлиника №1234» г.Орёл руководствоваться Регламентом Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области;
3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____/П.П.Петров /

Приложение №4
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ ОРЛОВСКОЙ ОБЛАСТИ «ПОЛИКЛИНИКА №1234» Г.ОРЁЛ

П Р И К А З

«___» _____2019 г. **№____**

О назначении Абонентов Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области.

Для выполнения служебных обязанностей с использованием сервисов и информационных систем Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области:

ПРИКАЗЫВАЮ:

1. Назначить Абонентами Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области:

Иванова Ивана Ивановича - инженера АСУ БУЗ Орловской области «Поликлиника №1234»

Петрова Петра Петровича – инженера АСУ БУЗ Орловской области «Поликлиника №1234»

2. В своей работе Абонентам Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области руководствоваться Регламентом Защищённой виртуальной сети №1322 ViPNet Департамента здравоохранения Орловской области;

3. Контроль за исполнением приказа оставляю за собой.

Главный врач _____/П.П.Петров /

Приложение №5
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

Соглашение
о неразглашении персональных данных субъекта

Я, Иванов Иван Иванович, понимаю, что получаю доступ к персональным данным. Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных. Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный. В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать требования законодательства Российской Федерации в области защиты персональных данных. Я подтверждаю, что не имею права разглашать:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о состоянии здоровья;
- сведения о заработной плате;
- сведения о социальных льготах;
- сведения о занимаемой должности;
- сведения о наличии судимостей;
- адрес места жительства;
- домашний телефон;
- сведения о месте работы или учебы членов семьи и родственников;

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты, я несу ответственность в соответствии с действующим законодательством.

"___"_____2019 г. _____

Приложение №6
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

Доверенность
на получение дистрибутива ключей

(*наименование населенного пункта*) «_____»_____2019 г.

Бюджетное учреждение здравоохранения Орловской области «Поликлиника №1234» в лице главного врача Петрова Петра Петровича уполномочивает: Иванова Ивана Ивановича, паспорт 4700 123456, выданный Отделом УФМС России по Орловской области г.Орла 01.01.2017 г. получить дистрибутив ключей для первичного запуска прикладной программы сети ViPNet №1322.

Настоящая доверенность действительна по «___» _____ 2019 г.

Подпись лица, получившего доверенность _____

Главный врач _____ /Петров П.П./

Приложение №7
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

ЖУРНАЛ УЧЁТА ВЫДАЧИ КЛЮЧЕВЫХ ДОКУМЕНТОВ

№ п/п	Дата выдачи	Организация	Ф.И.О. пользователя	Идентификатор дистрибутива	Тип носителя
1	2	3	4	5	6

Способ передачи (нарочным, лично в руки, письмом ДП (рег.номер) в адрес…)	Подпись получившего (отправившего по ДП)	Отметка об уничтожении
7	8	9

Приложение №8
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

ЗАЯВКА
на изменение направлений связи и/или предоставления доступа к информационным системам Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области

Полное наименование организации без сокращений (на основании учредительных документов)	*Бюджетное учреждение здравоохранения Орловской области «Поликлиника №1234» г. Орёл*
Сокращённое название организации	*БУЗ Орловской области «Поликлиника №1234»*
Направления связи для организации защищённого обмена информацией	*- БУЗ Орловской области «Медицинский информационно – аналитический центр»;* *- ТФОМС Орловской области.*
Перечень информационных систем, к которым необходим доступ:	*ЕРИС «Льготное лекарственное обеспечение населения Орловской области»*
Контактный телефон Локального администратора	
Контактный e-mail Локального администратора	

_____ _____/_____

Дата ФИО / Подпись

Приложение №9
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

ПРОТОКОЛ
установления межсетевого взаимодействия

«____» _____ 2019 г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организаций
№_____	*Полное наименование организации*
№_____	*Полное наименование организации*

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 специалистом, уполномоченным 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. При установлении межсетевого взаимодействия в части ЭЦП, были произведены импорты справочников ЭЦП главных абонентов сети №___ и №___.
8. Смена межсетевых ключей, изменение состава АП, 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] [Делова почта] с указанием производимых изменений.
9. Стороны обязуются без предварительного согласия не производить изменений в настройках и структуре защищённых сетей, могущих привести к нарушению межсетевого взаимодействия.

Администратор сети ViPNet №1322	Администратор сети ViPNet №1322
(ФИО)	(ФИО)
(подпись)	(подпись)
«_____»_____2019 г.	«_____»_____2019 г.
М.П.	М.П.

Приложение №10
К Регламенту Защищённой виртуальной сети
ViPNet №1322 Департамента здравоохранения
Орловской области

ЗАЯВКА
на изменение Локального администратора и/или зарегистрированных Абонентов Защищённой виртуальной сети ViPNet №1322 Департамента здравоохранения Орловской области «Медицинский информационно – аналитический центр»

Полное наименование организации без сокращений (на основании учредительных документов)	*Бюджетное учреждение здравоохранения Орловской области «Поликлиника №1234» г. Орёл*
Сокращённое название организации	*БУЗ Орловской области «Поликлиника №1234»*
ФИО Абонента зарегистрированного на Абонентском пункте	*БУЗ Орловской области «Поликлиника №1234» – 1: Иванов Иван Иванович* *БУЗ Орловской области «Поликлиника №1234» – 2: Петров Петр Петрович*
ФИО Локального администратора	*Иванов Иван Иванович*
Контактные телефоны Локального администратора	*(4862) 88-88-88*
Контактный E-mail Локального администратора	ivanov@mail.ru

_____ _____/_____
Дата ФИО / Подпись