МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
РЕСПУБЛИКИ СЕВЕРНАЯ ОСЕТИЯ-АЛАНИЯ

ПРИКАЗ

«03» апреля 2018 г. № 269 о/д

г. Владикавказ

Об организации защищенного подключения медицинских организаций Республики Северная Осетия-Алания к ведомственной защищённой сети передачи данных в сфере охраны здоровья Министерства здравоохранения Республики Северная Осетия-Алания с использованием криптографических шлюзов (ViPNet, АПКШ «Континент») для реализации работы в Единой медицинской информационно-аналитической системе

В рамках обеспечения требований к информационной безопасности при работе сотрудников Министерства здравоохранения Республики Северная Осетия - Алания и сотрудников медицинских организаций Республики Северная Осетия-Алания с Единой медицинской информационно-аналитической системой Республики Северная Осетия-Алания (далее - ЕМИАС)

п р и к а з ы в а ю:

1.Утвердить Положение о ведомственной защищенной сети передачи данных в сфере охраны здоровья Министерства здравоохранения Республики Северная Осетия - Алания (далее – ВЗСПД МЗ РСО-А).

2.Назначить государственное бюджетное учреждение здравоохранения «Республиканский медицинский информационно-аналитический центр» Министерства здравоохранения Республики Северная Осетия – Алания (далее - ГБУЗ «РМИАЦ» МЗ РСО-А) оператором ВЗСПД МЗ РСО-А.

3.Руководителям медицинских организаций Республики Северная Осетия - Алания, выполнить процедуры подключения и регистрации, описанные в Положении о ВЗСПД МЗ РСО-А (Приложение № 1) для получения доступа к ЕМИАС.

4.Директору ГБУЗ «РМИАЦ» МЗ РСО-А предоставить доступ для подключения Министерства здравоохранения Республики Северная Осетия - Алания и медицинских организаций Республики Северная Осетия - Алания к ЕМИАС при соблюдении ими требований, описанных в Положении о ВЗСПД МЗ РСО-А (Приложение № 1).

5.Директору ГБУЗ «РМИАЦ» РСО-А обеспечить бесперебойную работу и техническое обслуживание серверного и сетевого оборудования размещенного в центре обработки данных Министерства здравоохранения Республики Северная Осетия-Алания.

6.Контроль за исполнением настоящего приказа оставляю за собой.

Министр М. Ратманов

Приложение №1
к приказу
Министерства здравоохранения
Республики Северная Осетия-Алания
от 03.04.18г № 269 о/д

ПОЛОЖЕНИЕ
О ВЕДОМСТВЕННОЙ ЗАЩИЩЕННОЙ СЕТИ ПЕРЕДАЧИ ДАННЫХ В СФЕРЕ ОХРАНЫ ЗДОРОВЬЯ

г. Владикавказ
2018 г.

Содержание

1. Термины и определения

1.1. Список сокращений

АП	абонентский пункт
АРМ	автоматизированное рабочее место
ВЗСПДЗ РСО-А	ведомственная защищенная сеть передачи данных в сфере охраны здоровья
ИБ	информационная безопасность
ИС	информационная система
ЛВС	локальная вычислительная сеть
МО	медицинские организации
ОС	операционная система
ПАК	программно-аппаратный комплекс
ПО	программное обеспечение
СЗИ	средства защиты информации
СКЗИ	средства криптографической защиты информации (программные и программно-аппаратные)
СУ	сетевой узел
ТС	технические средства
УД	узел доступа
ФСБ	Федеральная служба безопасности РФ
ФСТЭК	Федеральная служба по техническому и экспортному контролю РФ
ЦОД	центр обработки данных
ЦУС	центр управления сетью
ЛВС	локальная вычислительная сеть

1.2. Термины и определения

Абонентский пункт	Персональный компьютер с установленным программным обеспечением «Континент-АП» либо ViPNet Клиент, входящий в состав ВЗСПДЗ РСО-А.
Абонент ВЗСПДЗ РСО-А	Юридическое лицо, являющееся оператором информации, формирующейся и обрабатываемой в процессе деятельности учреждений здравоохранения и других организаций Республики Северная Осетия Алания, подключенных к ВЗСПДЗ РСО-А в установленном порядке.
Администратор ВЗСПДЗ РСО-А	Должностное лицо Оператора, осуществляющее техническое обслуживание и администрирование компонентов ВЗСПДЗ РСО-А, находящихся в сегменте Оператора.
Администратор безопасности Абонента	Должностное лицо Абонента (Юридическое лицо либо индивидуальный предприниматель при наличии договора на сопровождение или сотрудник организации), осуществляющее администрирование информационных ресурсов и контроль эксплуатации компонентов ВЗСПДЗ РСО-А, находящихся в сегменте Абонента.
ВЗСПДЗ РСО-А	Виртуальная, наложенная на физические каналы связи защищенная транспортная сеть, построенная с использованием технологий АПКШ «Континент» или ViPNet CUSTOM, реализованная сертифицированными в установленном порядке средствами защиты информации.
Компонент ВЗСПДЗ РСО-А	Сетевые узлы, обеспечивающее функционирование ВЗСПДЗ РСО-А, и представляющие собой АПКШ «Континент» либо ViPNet Координатор или рабочее место с установленным ПО «Континент-АП» либо ViPNet Клиент.
Оператор ВЗСПДЗ РСО-А	Организация, осуществляющая координацию действий Абонентов ВЗСПДЗ РСО-А.
Оператор связи	Юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании лицензии.
ПАК Координатор	Программно-аппаратный комплекс, выполняющий функции межсетевого экрана и крипто маршрутизатора, имеющий сертификат соответствия ФСТЭК РФ и ФСБ РФ.

Пользователь ВЗСПДЗ РСО-А.	Должностное лицо Абонента, использующее для выполнения своих служебных обязанностей информационные системы и сервисы ВЗСПДЗ РСО-А.
Сетевой узел	Узел, подключаемый посредством АПКШ «Континент-АП» либо ПАК ViPNet Координатор к ВЗСПДЗ РСО-А.
Центр управления сетью	Аппаратные или программные средства для мониторинга, конфигурирования и управления компонентами ВЗСПДЗ.

2. Общие положения

2.1. Настоящее Положение разработано в соответствии со следующими нормативными правовыми актами:

– 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 ФАПСИ №152 от 13 июня 2001 года «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»;

– Регламентом информационной безопасности при использовании программно-аппаратных средств комплекса ViPNet, ОАО «ИнфоТеКС», 2010г., ФРКЕ. 00029-04 90 01;

– Методическими рекомендациями Министерства здравоохранения Российской Федерации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения.

2.2. Настоящее Положение определяет и устанавливает:

– цели и задачи ведомственной защищенной сети передачи данных в сфере охраны здоровья (далее – ВЗСПДЗ РСО-А) государственного бюджетного учреждения здравоохранения Республики Северная Осетия Алания «Медицинский информационно-аналитический центр» (далее – Оператор);

– состав и устройство ВЗСПДЗ РСО-А;

– функции, полномочия и ответственность Оператора и Абонентов ВЗСПДЗ РСО-А (далее – Абоненты);

– функции и ответственность Администратора ВЗСПДЗ РСО-А и Администратора безопасности ВЗСПДЗ РСО-А;

– порядок назначения пользователей ВЗСПДЗ РСО-А;

– порядок подключения Абонентов к ВЗСПДЗ РСО-А;

– порядок организации защищённого межсетевого взаимодействия;

– требования, предъявляемые к организации работы ВЗСПДЗ РСО-А.

3. Присоединение и отзыв заявления о присоединении к Положению

3.1. В целях присоединения к Положению Абонент направляет Оператору Заявление о присоединении к порядку подключения к ВЗСПДЗ, указанной в Приложении №7.

3.2. С момента регистрации Заявления о присоединении к Положению у Оператора Абонент, считается присоединившимся к Положению. Факт

присоединения Абонента к Положению является полным принятием им условий Положения и всех его приложений в редакции, действующей на момент регистрации Заявления о присоединении к Положению.

3.3. Оснований для отказа в приеме Заявления о присоединении к Положению не предусмотрено.

4. Внесение изменений (дополнений) в Положение

4.1. Внесение изменений (дополнений) в Положение осуществляется Оператором в одностороннем порядке.

4.2. Изменения в Положение вносятся приказом Оператора.

4.3. Все приложения, изменения и дополнения к Положению являются его составной и неотъемлемой частью.

4.4. Все изменения (дополнения), вносимые в Положение по инициативе Оператора и не связанные с изменением действующего законодательства Российской Федерации вступают в силу и становятся обязательными по истечении 5 (пяти) календарных дней со дня издания приказа.

4.5. Все изменения (дополнения), вносимые в Положение в связи с изменением действующего законодательства Российской Федерации вступают в силу одновременно с вступлением в силу изменений (дополнений) указанных в нормативных правовых актах действующего законодательства. Все изменения (дополнения) в Положение с момента вступления в силу равно распространяются на всех Абонентов, присоединившихся к Положению ранее даты вступления изменений (дополнений) в силу.

4.6. В случае несогласия с изменениями (дополнениями) Абонент имеет право до вступления в силу таких изменений (дополнений) подать Отзыв заявления о присоединении к Положению на бумажном носителе.

5. Отзыв заявления о присоединении

5.1. В случае необходимости отзыва Абонентом Заявления о присоединении к Положению Оператор письменно уведомляется за 30 (тридцать) календарных дней до даты отзыва по форме, указанной в Приложении №6 к Положению.

6. Назначение, задачи и состав ВЗСПДЗ РСО-А

6.1. ВЗСПДЗ РСО-А предназначена для организации защищенного информационного обмена между Оператором и Абонентами.

6.2. Основными задачами, которые решает ВЗСДПЗ РСО-А, являются:

– уменьшение вероятности потери, искажения и хищения информации при её передаче по каналам связи;

– выполнение требований законодательства в области обработки персональных данных в части защиты каналов связи;

– организация защищённого доступа к информационным системам (далее – ИС) и сервисам.

6.3. Состав ВЗСПДЗ РСО-А:

– ВЗСПДЗ РСО-А представляет собой территориально распределённую информационно-телекоммуникационную сеть, объединяющую Абонентов посредством технологии АПКШ «Континент» или ViPNet;

– центр управления сетью (далее – ЦУС) расположен у Оператора;

– связь абонентских пунктов (далее – АП) Абонентов осуществляется по каналам связи, которые используются Абонентами.

6.4. АП– IBM-совместимый компьютер, соответствующий следующим требованиям:

– процессор не менее intel core 2 duo;

– оперативная память не менее 1024 Мбайт;

– наличие сетевого интерфейса для соединения с сетью;

– наличие источника бесперебойного питания;

– установленная операционная система, Windows Server 2003 (32 бит), Windows Vista (32/64 бит), Windows Server 2008 (32/64 бит), Windows 7 (32/64 бит), Windows Server 2008 R2, Windows 8 или Windows 10, Linux;

– установлено программное обеспечение «Континент-АП» или ViPNet Клиент (далее – ViPNet Клиент).

7. Требования, предъявляемые к компонентам ВЗСПДЗ РСО-А при использовании программно-аппаратного комплекса ViPNet

7.1. Требования к программно-аппаратному комплексу ViPNet Координатор (далее – ViPNet Координатор).

7.1.1. Вводимый в эксплуатацию, а также эксплуатируемый ViPNet Координатор должны:

– иметь действующий сертификат соответствия удостоверяющий, что ViPNet Координатор соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от несанкционированного доступа (далее – НСД) в информационных и телекоммуникационных системах органов государственной власти РФ;

– иметь действующий сертификат соответствия удостоверяющий, что ViPNet Координатор соответствует требованиям ГОСТ 28147-89 и требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС3 и может использоваться для криптографической защиты (шифрование и имитозащита данных, передаваемых в IP-пакетах по сети связи общего пользования) информации, не содержащей сведений, составляющих государственную тайну;

– иметь действующий сертификат соответствия удостоверяющий, что ПАК защиты информации «ViPNet Coordinator HW» соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 3 уровню контроля и технических условий.

– быть подключены к исправному источнику бесперебойного питания.

7.2. Требования к размещению ViPNet Координатора.

7.2.1. ViPNet Координатор необходимо располагать в запираемом на ключ телекоммуникационном шкафу или стойке для сетевого оборудования.

7.2.2. Если ViPNet Координатор установлен в стойке для сетевого оборудования, которая находится не в серверной, то необходимо обеспечить запирание на ключ помещения, в котором расположено устройство.

7.3. Требования к АП.

7.3.1. Вводимый в эксплуатацию, а также эксплуатируемый АП должен:

– иметь действующий сертификат соответствия удостоверяющий, что программный комплекс ViPNet Client 3.2 КС3 соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от НСД в информационных и телекоммуникационных системах органов государственной власти РФ;

– иметь действующий сертификат соответствия удостоверяющий, что программный комплекс ViPNet Client 3.2 КС3 (варианты исполнения 1, 2) соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от НСД в информационных и телекоммуникационных системах органов государственной власти РФ;

– иметь действующий сертификат соответствия ФСТЭК удостоверяющий, что программный комплекс «ViPNet CUSTOM 3.2» соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 3 уровню контроля, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищенности;

– быть подключен к исправному источнику бесперебойного питания.

7.4. Требования к размещению АП.

7.4.1. АП необходимо размещать в помещении таким образом, чтобы был исключен просмотр экрана АП посторонними лицами, а также сотрудниками, не являющимися пользователями данного АП.

7.5.Требования к рабочим местам пользователей, подключаемым к ViPNet Координатор.

7.5.1. Рабочее место пользователя, подключаемое к ViPNet Координатор должно быть:

– подключено к исправному источнику бесперебойного питания.

7.6. Требования к наличию IP-адресов, маршрутизируемых в сеть Интернет.

7.6.1.IP-адрес, маршрутизируемый в сеть Интернет, присваивается интерфейсу ViPNet Координатора Абонента при схеме подключения, представленной на рисунке 1.

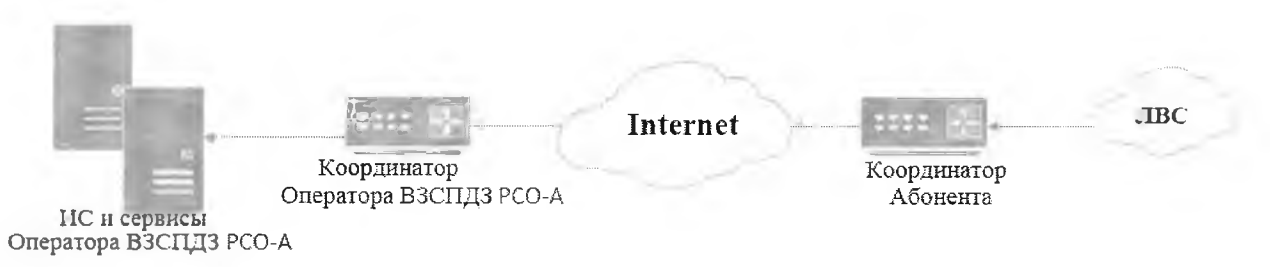

Рисунок 1 – Схема подключения, предполагающая наличие IP-адреса, маршрутизируемого в сеть Интернет, на интерфейсе ViPNet Координатора Абонента

7.6.2.IP-адрес, маршрутизируемый в сеть Интернет, присваивается интерфейсу сетевого оборудования Абонента при схеме подключения, представленной на рисунке 2. При этом сетевое оборудование Абонента может выступать в качестве маршрутизирующего устройства.

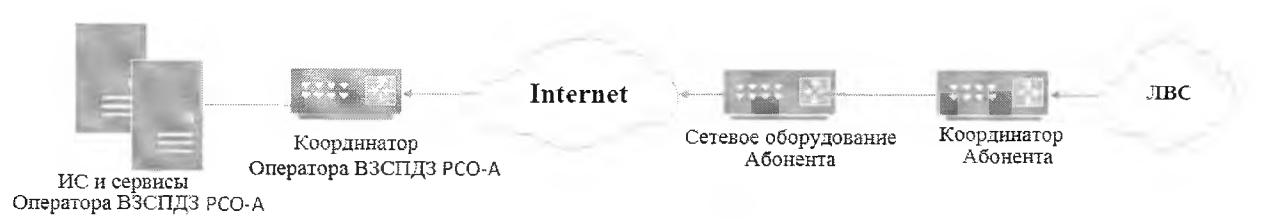

Рисунок 2 – Схема подключения, предполагающая наличие IP-адреса, маршрутизируемого в сеть Интернет, на интерфейсе сетевого оборудования Абонента

8. Требования, предъявляемые к компонентам ВЗСПДЗ РСО-А при использовании программно-аппаратного комплекса «Континент»

8.1. Требования к аппаратно-программному комплекс шифрования «Континент»

8.1.1. Вводимый в эксплуатацию, а также эксплуатируемый АПКШ «Континент» должен иметь сертификаты соответствия:

- ФСТЭК России №1905 от 10.09.2009г., является программно-техническим средством защиты от несанкционированного доступа к информации, предназначен для построения виртуальных частных сетей (VPN) на основе глобальных сетей общего пользования, использующих протоколы семейства TCP/IP и соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) - по 3 классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 3 уровню контроля, и может использоваться для создания автоматизированных систем до класса защищенности 1В включительно и при создании информационных систем персональных данных до 1 класса включительно при условии выполнения ограничений, указанных в технических условиях;

- ФСБ России № СФ/525-1352 от 21.07.2009г., соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от несанкционированного доступа в информационно-телекоммуникационных систем органов государственной власти Российской Федерации;

- ФСБ России № СФ/124-1474 от 09.05.2010г., соответствует требованиям ФСБ России к средствам криптографической защиты информации класса КС2 и может использоваться для криптографической защиты (генерация ключевой информации, управление ключевой информацией, шифрование и имитозащита данных, передаваемых в IP пакетах по общим сетям передачи данных) информации, не содержащей сведений, составляющих государственную тайну.

8.2 Требования к размещению АПКШ «Континент».

8.2.1. АПКШ «Континент» необходимо располагать в запираемом на ключ телекоммуникационном шкафу или стойке для сетевого оборудования.

8.2.2. Если АПКШ «Континент» установлен в стойке для сетевого оборудования, которая находится не в серверной, то необходимо обеспечить запирание на ключ помещения, в котором расположено устройство.

8.3. Требования к АП.

8.3.1. Вводимый в эксплуатацию, а также эксплуатируемый АП должен:

– иметь действующий сертификат соответствия удостоверяющий, что программный комплекс СКЗИ «Континент-АП» соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от НСД в информационных и телекоммуникационных системах органов государственной власти РФ;

– иметь действующий сертификат соответствия удостоверяющий, что программный комплекс СКЗИ «Континент-АП» (варианты исполнения 1, 2) соответствует требованиям ФСБ России к устройствам типа межсетевые экраны 4 класса защищенности и может использоваться для защиты информации от НСД в информационных и телекоммуникационных системах органов государственной власти РФ;

– иметь действующий сертификат соответствия ФСТЭК удостоверяющий, что программный комплекс СКЗИ «Континент-АП» соответствует требованиям руководящих документов «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 3 уровню контроля, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по 3 классу защищенности;

– быть подключен к исправному источнику бесперебойного питания.

8.4. Требования к размещению АП.

8.4.1. АП необходимо размещать в помещении таким образом, чтобы был исключен просмотр экрана АП посторонними лицами, а также сотрудниками, не являющимися пользователями данного АП.

8.5. Требования к рабочим местам пользователей, подключаемым к АПКШ «Континент».

8.5.1. Рабочее место пользователя, подключаемое к АПКШ «Континент» должно быть:

– подключено к исправному источнику бесперебойного питания.

8.6. Требования к наличию IP-адресов, маршрутизируемых в сеть Интернет.

8.6.1. IP-адрес, маршрутизируемый в сеть Интернет, присваивается интерфейсу АПКШ «Континент» Абонента при схеме подключения, представленной на рисунке 3.

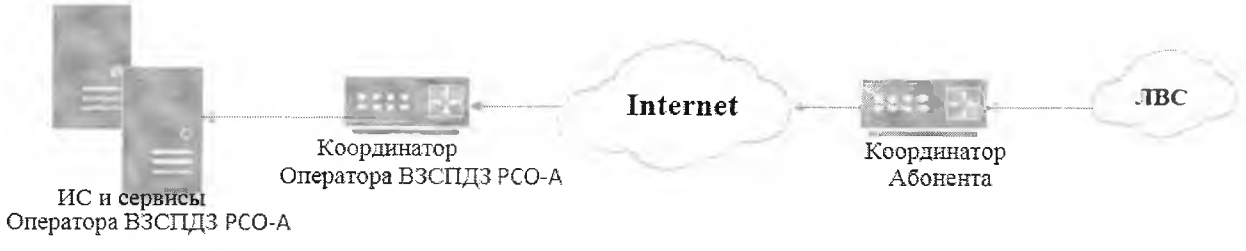

Рисунок 3 – Схема подключения, предполагающая наличие IP-адреса, маршрутизируемого в сеть Интернет, на интерфейсе АПКШ «Континент» Абонента

8.6.2. IP-адрес, маршрутизируемый в сеть Интернет, присваивается интерфейсу сетевого оборудования Абонента при схеме подключения, представленной на рисунке 4. При этом сетевое оборудование Абонента может выступать в качестве маршрутизирующего устройства.

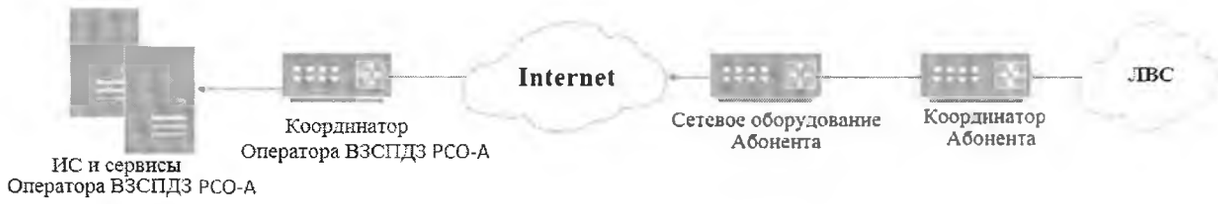

Рисунок 4 – Схема подключения, предполагающая наличие IP-адреса, маршрутизируемого в сеть Интернет, на интерфейсе сетевого оборудования Абонента

9. Эксплуатация компонентов ВЗСПДЗ РСО-А

Эксплуатация – проверка сетевой связности и работоспособности, каблирование, переключение режима работы оборудования, не требующее использования привилегированного доступа к оборудованию, в целях обеспечения бесперебойной работы компонентов ВЗСПДЗ РСО-А без изменения их конфигурации.

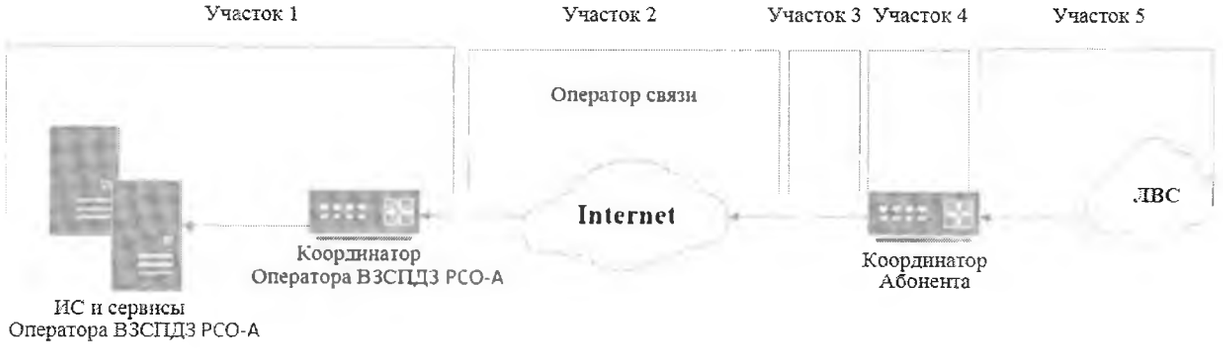

Рисунок 5 – Зоны ответственности Оператора и Абонента при подключении через Internet (Схема 1)

Таблица 1 – Разграничение зон ответственности при эксплуатации ВЗСПДЗ РСО-А согласно подключению по Схеме 1

№ Участка	Оператор	Абонент
1	X	
2	Оператор связи	
3		X
4		X
5		X

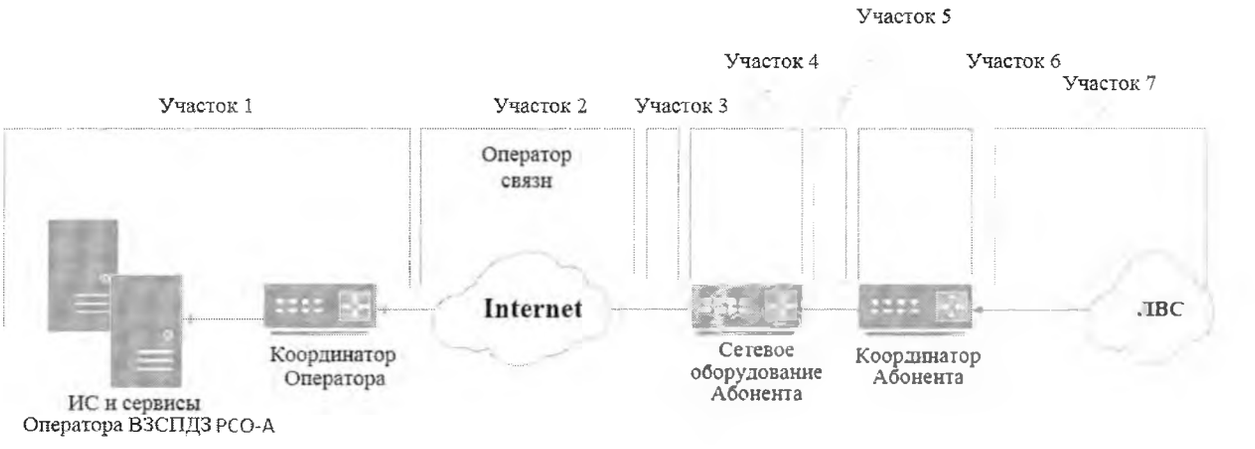

Рисунок 6 – Зоны ответственности Оператора и Абонента при подключении через Internet с использованием дополнительного сетевого оборудования (Схема 2)

Таблица 2 – Разграничение зон ответственности при эксплуатации ВЗСПДЗ РСО-А согласно подключению по Схеме 2

№ Участка	Оператор	Абонент
1	X	
2	Оператор связи	
3		X
4		X
5		X
6		X
7		X

10. Функции, полномочия и ответственность Оператора

10.1. Оператор выполняет следующие функции:

– рассмотрение заявлений Абонентов на подключение к ВЗСПДЗ РСО-А;

– осуществление подключения к ВЗСПДЗ РСО-А новых Абонентов, в соответствии с заявлениями на подключение.

10.2. Полномочия Оператора:

– информировать руководителей Абонентов при невыполнении их сотрудниками требований безопасности и несоблюдения других требований по обеспечению бесперебойного функционирования ВЗСПДЗ РСО-А;

– принимать решение об отключении или ограничении доступа к ИС и сервисам ВЗСПДЗ РСО-А в случаях нарушения пользователями Абонента требований настоящего Положения;

– проводить проверки компонентов ВЗСПДЗ РСО-А Абонентов (в том числе выездные) с целью выявления фактов несоблюдения требований настоящего Положения.

10.3 Ответственность Оператора.

Оператор ВЗСПДЗРСО-А несёт ответственность за:

– невыполнение функций, возложенных на него данным Положением;

– невыполнение требований настоящего Положения и нормативных правовых актов в области защиты информации.

11. Функции, полномочия и ответственность Абонента

11.1.Абонент выполняет следующие функции:

– проводит оснащение необходимым программным обеспечением (далее – ПО) и оборудованием для соответствия АП и АПКШ «Континент» либо ViPNet Координатор требованиям настоящего Положения;

– предоставляет Оператору документы на компоненты ВЗСПДЗ РСО-А.

11.2.Полномочия Абонента:

– назначать и утверждать приказом Администраторов безопасности ВЗСПДЗ РСО-А (Приложение №2);

– назначать и утверждать приказом перечень сотрудников (Пользователей), которым для выполнения служебных обязанностей необходим доступ к ИС и сервисам ВЗСПДЗ РСО-А (Приложение №3).

11.3.Абонент несет ответственность за:

– невыполнение требований настоящего Положения и нормативных правовых актов в области защиты информации;

– использование АПКШ «Континент» либо ViPNet Координатор и ViPNet Клиент или СКЗИ «Континент-АП» с истекшим сроком действия сертификатов соответствия, выданных ФСБ и ФСТЭК;

– отсутствие подключения АП и АПКШ «Континент» либо ViPNet Координатор к исправным источникам бесперебойного питания.

– абонент несёт ответственность за соответствие схемы подключения АРМ к защищённой сети и отсутствие нерегламентированных подключений стороннего оборудования и компонентов ЛВС в защищённую сеть. При наличии 2-х физически сетевых интерфейсов на АРМ абонент обязан использовать только один из них. При этом второй интерфейс должен быть опечатан и программно отключен.

12. Порядок назначения пользователей ВЗСПДЗ РСО-А

12.1. Для выполнения функций по администрированию ВЗСПДЗ РСО-А, приказом руководителя Оператора назначаются Администраторы ВЗСПДЗ РСО-А.

12.2. Для доступа к работе с ИС и сервисами ВЗСПДЗ РСО-А приказами руководителей Оператора и Абонента назначаются сотрудники (Пользователи), которым для выполнения служебных обязанностей необходим доступ к указанным выше ресурсам.

12.3. В случае изменения перечня Пользователей Администратор безопасности Абонента обязан информировать Оператора в течение 5 (пяти) рабочих дней.

Необходимо направить оператору сведения с указанием ФИО, должности пользователя, списка ИС (в которых он работал или к которым ему предоставляется доступ), причины изменения (предоставление/прекращение/изменение).

12.4. В случае смены должностного лица (юридическое лицо либо индивидуальный предприниматель при наличии договора на сопровождение или сотрудник организации), на которого возложены функции Администратора безопасности, руководитель Абонента обязан в течение 5 (пяти) рабочих дней известить об этом Оператора в письменной форме.

13. Роли и функции пользователей ВЗСПДЗ РСО-А

13.1. Администратор Оператора выполняет следующие функции:

– разработка предложений по внедрению компонентов ВЗСПДЗ РСО-А;

– администрирование компонентов ВЗСПДЗ РСО-А согласно таблицам в Приложении;

– контроль за соблюдением всеми категориями пользователей правил работы и использования компонентов ВЗСПДЗ РСО-А;

– создание новых АП ВЗСДПЗ РСО-А;

– формирование и выдача дистрибутивов ключей для АП Абонентов доверенным способом;

– восстановление конфигурации ViPNet-Координатор либо ЦУС АПКШ «Континент» на стороне оператора в случае сбоев;

– проверка доступности АПКШ «Континент» либо ViPNet-Координатор, расположенных у Абонента;

– рассылка обновлённых справочников, парольной и ключевой информации Абонентам;

– организация межсетевого взаимодействия.

– настройка и перенастройка ЦУС АПКШ «Континент» либо ViPNet-Координатор для работы как в составе отказоустойчивого кластера (failover) так и без такового (single), на работу через различные каналы связи;

– добавление новых связей между АП Абонента и ЦУС АПКШ «Континент» либо ViPNet-Координатор Абонента для организации защищённого обмена информации, в случае если у Абонента имеются территориально разнесённые филиалы;

– поддержание в работоспособном состоянии компонентов ВЗСПДЗ РСО-А, установленных у Оператора.

13.2. Полномочия Администратора Оператора ВЗСПДЗ РСО-А:

– получение от Абонентов необходимых сведений об использовании ими ВЗСПДЗ РСО-А.

– периодический контроль соответствия настроек сетевого оборудования Абонента в соответствии с требованиями к информационной безопасности.

– проводить внеплановые проверки состояния физической инфраструктуры ЛВС Абонента для выявления нерегламентированных подключений к защищённому сегменту ЛВС нарушающих требования защиты информации.

– -использовать программные средства для выявления нерегламентированных подключений и некорректной настройки оборудования абонента

Администратор абонента несёт ответственность за изменения в схеме ЛВС абонента, не соответствующие указанной схеме подключения и повышающие риск компрометации персональных данных.

13.3. Администратор Оператора ВЗСПДЗ РСО-А несет ответственность за:

– за невыполнение требований технической и эксплуатационной документации на компоненты ВЗСПДЗ РСО-А;

– невыполнение требований настоящего Положения и нормативных правовых актов в области защиты информации;

– соблюдение конфиденциальности информации, полученной в связи с выполнением своих обязанностей.

13.4. Администратор безопасности Абонента ВЗСПДЗ РСО-А.

13.5. Зоной ответственности Администратора безопасности Абонента является ЛВС Абонента, в которой расположены и подключены компоненты

ВЗСПДЗ РСО-А, Пользователям которой предоставляется доступ к ИС и сервисам ВЗСПДЗ РСО-А.

13.6. Администратор безопасности выполняет следующие функции:

– контроль эксплуатации компонентов ВЗСПДЗ РСО-А, установленных у Абонента;

– установка модуля СКЗИ «Континент-АП» либо ViPNet Клиент [Монитор] на АП в 3 (третий) режим в качестве штатного режима функционирования;

– контроль соблюдения Пользователями Абонента конфиденциальности при обращении со сведениями о функционировании и порядке обеспечения безопасности применяемых компонентов ВЗСПДЗ РСО-А и ключевых документах к ним, которые им доверены или стали известны в процессе работы в ВЗСПДЗ РСО-А;

– ознакомление Пользователей Абонента с правилами работы, требованиями безопасности ВЗСПДЗ РСО-А и ответственностью за нарушение данного Положения;

– инструктирование Пользователей Абонента по вопросам работы с сервисами и ИС ВЗСПДЗ РСО-А;

– поддержание в работоспособном состоянии компонентов ВЗСПДЗ РСО-А, установленных у Абонента;

– эксплуатация и хранение средств криптографической защиты информации (далее – СКЗИ), технической и эксплуатационной документации, ключевых документов, носителей информации ограниченного распространения относящихся к компонентам ВЗСПДЗ РСО-А в соответствии с требованиями действующего законодательства;

– уведомление руководителей Абонента и Оператора о действиях Пользователей, осуществивших несанкционированный доступ (далее – НСД) к ИС и сервисам ВЗСПДЗ РСО-А или нарушивших другие требования по обеспечению безопасности информации и бесперебойной работы ВЗСПДЗ РСО-А;

– уведомление руководителя Абонента о необходимости обновления сертификатов соответствия, выданных ФСБ и ФСТЭК на СКЗИ, в случае истечения их срока действия.

13.7. Администратору безопасности запрещается:

13.7.1. Использовать СКЗИ при компрометации ключей, скрывать факт компрометации ключей.

13.7.2. Использовать СКЗИ с истекшим сроком действия сертификатов соответствия, выданных ФСБ и ФСТЭК на данное СКЗИ.

13.7.3. Допускать к подключенному к ВЗСПДЗ РСО-А рабочему месту посторонних лиц.

13.7.4. Самостоятельно проводить изменения в настройках ПОСКЗИ «Континент-АП» либоViPNet-клиент.

13.7.5. Передавать пароли и ключевую информацию третьим лицам, а также размещать их в местах, доступных посторонним.

13.8. Администратор безопасности несет ответственность:

13.8.1. За невыполнение требований настоящего Положения, нормативных правовых актов в области защиты информации, а также требований других актов, регулирующих работу ВЗСПДЗ РСО-А.

13.8.2. За невыполнение требований технической и эксплуатационной документации на компоненты ВЗСПДЗ РСО-А.

13.8.3. За соблюдение конфиденциальности информации, полученной в связи с выполнением своих обязанностей в рамках действующего законодательства.

13.8.4. За поддержание в работоспособном состоянии компонентов ВЗСПДЗ РСО-А, установленных у Абонента.

13.9. Пользователь абонента ВЗСПДЗ РСО-А.

13.9.1. Пользователь обязан:

– соблюдать конфиденциальность информации, полученной в связи с выполнением своих должностных обязанностей.

– при работе с ИС и сервисами ВЗСПДЗ РСО-А выполнять только задания, связанные с должностными обязанностями;

– при выявлении вредоносных программ или признаков нештатного функционирования компонентов ВЗСПДЗ РСО-А немедленно сообщить Администратору безопасности;

– обеспечивать безопасность хранения ключевой информации и (или) пароля.

13.9.2. Пользователю запрещается:

– оставлять свое рабочее место, подключенное к ВЗСПДЗ РСО-А во включенном состоянии без контроля и с незаблокированными устройствами ввода и отображения информации;

– допускать к АП, подключенному к ВЗСПДЗ РСО-А, посторонних лиц;

– самостоятельно проводить изменения в настройках СКЗИ «Континент-АП» либоViPNet-Клиент;

– передавать пароли и ключевую информацию третьим лицам, а также размещать их в местах, доступных посторонним.

13.9.3. Пользователь несет ответственность за:

– невыполнение требований настоящего Положения;

– соблюдение конфиденциальности информации, полученной в связи с выполнением своих обязанностей в рамках действующего законодательства.

14. Порядок организации подключения Абонентов к ВЗСПДЗ РСО-А

14.1. Подключение Абонентов к ВЗСПДЗ РСО-А организуется как по решению Оператора, так и самостоятельно по инициативе нового Абонента.

14.2. Организация подключения новых Абонентов включает в себя следующие этапы:

– этап подачи заявления;

– этап рассмотрения заявления;

– этап подключения Абонента.

14.3. Абонент формирует и направляет Оператору пакет документов о намерении подключиться к ВЗСПДЗ РСО-А, с указанием цели подключения, перечня абонентов, с которыми необходима организация защищенного информационного обмена, либо перечня ИС и сервисов, к которым необходимо организовать доступ.

В комплект документов, передаваемый Абонентом входят:

– заявление на подключение к ВЗСПДЗ РСО-А (Приложение №1);

– копия приказа о назначении Администратора безопасности Абонента ВЗСПДЗ РСО-А (Приложение №2);[1]

– копия приказа о назначении Пользователей Абонента ВЗСПДЗ РСО-А (Приложение №3), в случае подключения к информационным ресурсам с использованием ПО СКЗИ «Континент-АП» либо ViPNet Клиент;[2]

– информация об адресации согласно схеме подключения (Приложение №5), в случае подключения ПАК ViPNet Координатор либо АПКШ «Континент».

14.4. Этап рассмотрения заявления.

14.4.1Оператор в течение 10 (десяти) рабочих дней с момента получения заявления принимает решение о целесообразности подключения нового Абонента к ВЗСПДЗ РСО-А.

14.4.2Приобретение ViPNet Клиент либо СКЗИ «Континент-АП» или АПКШ «Континент» либо ViPNet Координатор до рассмотрения заявления о намерении подключиться к ВЗСПДЗ РСО-А не является основанием и гарантией подключения Абонента к ВЗСПДЗ РСО-А.

14.4.3В случае отрицательного результата рассмотрения заявки, Оператор уведомляет Абонента об отказе в подключении к ВЗСПДЗ РСО-А с обоснованием причины отказа.

14.4.4В случае отсутствия замечаний по предоставленным документам, не позднее 10 (десяти) рабочих дней со дня получения комплекта документов, Оператор осуществляет процедуру оценки технической возможности и согласования схемы подключения нового Абонента.

14.5. Этап закупки программного или программно-аппаратного обеспечения.

14.5.1 Закупка ViPNet Клиент либо СКЗИ «Континент-АП» или АПКШ «Континент» либо ViPNet Координатор, обеспечение необходимым для подключения количеством лицензий, ключевых носителей информации осуществляется новым Абонентом самостоятельно. При оформлении документов на приобретение программных или аппаратных продуктов и

---

[1]Администраторами безопасности, необходимо назначать системных администраторов или программистов осуществляющих контроль эксплуатации СКЗИ ВЗСПДЗ РСО-А в МО.

[2] Допускать к самостоятельной работе с СКЗИ необходимо непосредственно тех сотрудников, которые работают на данном рабочем месте.

лицензий новый Абонент указывает регистрационный номер сети ViPNet №3223.

14.6. Этап подключения Абонента.

14.6.1 Подключение нового Абонента осуществляется с использованием программного или программно-аппаратного обеспечения ViPNet либо Континент.

14.6.2Сроки установки ПО ViPNet Клиент либо СКЗИ «Континент-АП» или АПКШ «Континент» либо ViPNet Координатор нового Абонента согласовываются новым Абонентом и Оператором ВЗСПДЗ РСО-А.

14.6.3Оператор ВЗСПДЗ РСО-А в согласованные с новым Абонентом сроки:

– выполняет регистрацию СУ в ЦУС;

– организует основные направления связи между СУ, в соответствии с заявкой на подключение;

– формирует необходимую справочную и ключевую информацию;

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

– уведомляет Администратора безопасности Абонента, по контактной информации, указанной в заявлении, о завершении обозначенных работ. Для получения дистрибутива ключей и пароля доступа к Оператору ВЗСПДЗ РСО-А направляется Администратор безопасности с доверенностью на получение дистрибутива ключей (Приложение №4).

14.6.4Факт выдачи дистрибутива ключей заносится в Журнал поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов (Приложение №15).

15. Требования к настройки ЛВС и АРМ абонента

15.1 Настройка маршрутизатора абонента

Для настройки подключения к оператору связи ВЗСПДЗ РСО-А администратору абонента необходимо заполнить форму заявления (Приложение №10, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru) и передать подписанный руководителем бланк оператору ВЗСПДЗ РСО-А.

После рассмотрения заявки, в случае положительного решения, абоненту присваивается номер технологической площадки и передаются сведения:

- Диапазоны ip адресации.
- Учетные данные для формирования удаленного подключения и логины для удаленного доступа к оборудованию абонента.
- Параметры для настройки роутера (NTP, SNMP, OSPF, VLAN, адреса для удаленного контроля оборудования, требования к настройке сервисов DHCP и межсетевого экрана, условия для автоматического

переключения на резервного провайдера в аварийных ситуациях и обратного переключения при восстановлении основного канала связи)

После успешной настройки маршрутизатора администратором абонента, необходимо передать параметры авторизации оператору ВЗСПДЗ РСО-А для регистрации в системе мониторинга и контроля корректности настройки по форме (Приложение №11, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru).

Оператором ВЗСПДЗ РСО-А производится тестирование и проверка корректности настроек, после чего выдаётся разрешение на настройку коммутационного оборудования.

15.2 Настройка коммутаторов абонента.

Для настройки коммутаторов абонента необходимо подключить коммутатор к маршрутизатору и произвести настройки:

- VLAN (выданные в ответе на заявлении о регистрации маршрутизатора абонента);
- NTP (выданные в ответе на заявлении о регистрации маршрутизатора абонента);
- SNMP (выданные в ответе на заявлении о регистрации маршрутизатора абонента);
- portsecurity с блокировкой всех не разрешенных явно mac адресов;
- Отключение всех портов (за исключением транковых) до разрешения подключения АРМ;
- Учетных записей для контроля и администрирования оборудования.

После успешной настройки коммутатора абонента, администратору абонента необходимо передать данные для удаленного подключения, регистрации в системе мониторинга и контроля корректности настройки оператору ВЗСПДЗ РСО-А по форме (Приложение №11, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru).

Оператором ВЗСПДЗ РСО-А производится тестирование и проверка корректности настроек, после чего выдаётся разрешение на подключение АРМ.

Если используется маршрутизатор в закрытом сегменте сети, то должна отсутствовать NAT трансляция при транзите трафика через этот маршрутизатор на криптошлюз. Также запрещено подключение любых технических устройств или каналов связи к данному маршрутизатору или в сегменты сети за ним, через которые может быть осуществлён процесс передачи данных в обход криптошлюза.

В случае выявления данного нарушения, абонент отключается от сети оператора и должен повторно инициировать процесс получения доступа к ресурсам с заменой ответственного администратора безопасности. В данном случае до предоставления решения производится полный аудит физической и логической сети абонента для решения вопроса по его заявке.

15.3 Подключение АРМ:

- Для регистрации АРМ абонента оформить заявку с указанием необходимых данных (Приложение №12, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru).
- После получения положительного ответа, администратор абонента вводит АРМ в домен и сообщает о результате оператору ВЗСПДЗ РСО-А.

Оператор ВЗСПДЗ РСО-А производит проверку АРМ на соответствие требованиям, после чего применяет разрешающие политики для обеспечения работы данного АРМ. В случае некорректного именования или некорректного подключения АРМ оператор ВЗСПДЗ РСО-А вправе аннулировать регистрацию АРМ. При введении в сетевую инфраструктуру объекта с неверным именем ответственность за блокировку некорректного АРМ несёт администратор абонента. Для разблокировки компьютера администратору абонента необходимо сообщить неверное имя оператору ВЗСПДЗ РСО-А для его удаления и переустановить операционную систему на данном АРМ с установкой корректного имени.

15.4 Подключение к информационным ресурсам.

15.4.1 Подключение к информационным ресурсам защищённого сегмента сети с доступом к персональным и медицинским данным:

- Абоненту необходимо заполнить заявку на доступ к информационной системе (Приложение №13, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru).

15.4.2Подключение к информационным ресурсам без доступа к персональным и медицинским данным:

- Подключение к сети интернет с доступом по белому списку адресов осуществляется по заявке (Приложение №13, а также форму для массового заведения размещённую на сайте minzdrav-rso.ru).

16. Организация межсетевого взаимодействия

16.1 Для организации межсетевого взаимодействия между ВЗСПДЗ РСО-А и сторонней сетью Континент либо ViPNet Оператор сторонней Континент либо ViPNet сети готовит информационное письмо, в котором информируют другую сторону о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц ответственных за организацию межсетевого взаимодействия.

16.2 Для организации межсетевого взаимодействия между ВЗСПДЗ РСО-А и сторонней сетью ViPNet Операторами указанных сетей заключается соглашение об установлении межсетевого взаимодействия согласно Приложению № 8.

16.3 После заключения соглашения Администратор ВЗСПДЗ РСО-А и Администратор сторонней сети Континент либоViPNet выполняют формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные

межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой из сетей.

16.4 Начальный экспорт доверенным способом передается в соответствующие ЦУС, с которыми должно осуществляться межсетевое взаимодействие.

16.5 Во всех ЦУС выполняется ввод и обработка полученного из других ЦУС начального экспорта, установление связей своих АП с АП ЦУС, предоставившими информацию (ответный экспорт) для ЦУС, приславших первичную информацию, включая свои сертификаты.

16.6 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 выполняется в автоматическом режиме.

17 Компрометация ключевой информации АП

17.1 Под компрометацией ключей понимается утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

17.2 Ключи пользователя считаются скомпрометированными в следующих случаях:

– посторонним лицам мог стать доступным файл ключевого дистрибутива;

– посторонним лицам мог стать доступным съемный носитель с ключевой информацией;

– посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на компьютере, если все ключи хранятся на компьютере;

– на АП установлен СКЗИ «Континент-АП» либо ViPNet-Клиент [Монитор] в 4 или 5 режиме работы, и:

– в локальной сети возможно присутствие посторонних лиц или на границе локальной сети отсутствует (отключен) межсетевой экран;

– сменился Пользователь, на которого оформлен пароль и ключ.

17.3 К событиям, требующим проведения служебной проверки и принятия решения о компрометации ключевой информации, относится возникновение подозрений в утечке информации при ее передаче в ВЗСПДЗ РСО-А.

17.4 В случае прекращения полномочий Пользователя, ключи данного Пользователя считаются скомпрометированными и подлежат отзыву (аннулированию).

17.5 Администратор безопасности Абонента, в течение 1 (одного) рабочего дня, доводит информацию о факте компрометации (либо угрозе или предпосылке компрометации) до Оператора ВЗСПДЗ РСО-А.

17.6 Оператор ВЗСПДЗ РСО-А при получении информации о компрометации ключевой информации в течение 1 (одного) рабочего дня обязан организовать:

– объявление ключей АП скомпрометированными и создание справочников связей при компрометации с необходимой информацией;

– оповещение о факте компрометации ключей всех Пользователей, связанных с Пользователем, ключевая информация которого была скомпрометирована;

– формирование новой ключевой информации и рассылку сформированных обновлений ключей на рабочие места Пользователей ВЗСПДЗ РСО-А.

18 Порядок организации хранения и учета ключевой информации компонентов ВЗСПДЗ РСО-А

18.1 Хранение, эксплуатация и учет СКЗИ, ключевой информации компонентов ВЗСПДЗ РСО-А осуществляется в соответствии с требованиями действующего законодательства в области криптографической защиты информации.

18.2 Организация поэкземплярного учета СКЗИ и ключевой информации компонентов ВЗСПДЗ РСО-А Оператора осуществляется Администратором Оператора.

18.3 Организация поэкземплярного учета СКЗИ и ключевой информации компонентов ВЗСПДЗ РСО-А Абонента осуществляется Администратором безопасности Абонента.

18.4 Учет СКЗИ ведется в Журнале поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов в соответствии с Приложением №15.

18.5 Программные СКЗИ учитываются совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

18.6 Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под роспись в соответствующем Журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

18.7 Если эксплуатационной и технической документацией к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (на весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в техническом журнале (Приложение № 16), ведущемся непосредственно Администратором безопасности.

18.8 В состав ключевой информации компонентов ВЗСПДЗ РСО-А, входят следующие составляющие:

– дистрибутив справочно-ключевой информации – сборник, содержащий личные ключи пользователя, ключевой набор СУ и адресные справочник;

– личные ключи пользователя – ключи защиты пользователя, необходимые для его аутентификации на сетевом узле, и может содержать ключи подписи пользователя;

– резервный набор персональных ключей пользователя – предназначен для получения дистанционного обновления ключевой информации при изменении исходной ключевой информации в Удостоверяющем и ключевом центре.

18.9 Дистрибутив справочно-ключевой информации.

18.9.1 Дистрибутив справочно-ключевой информации формируется Администратором Оператором ВЗСПДЗ РСО-А и передается Администратору безопасности Абонента ВЗСПДЗ РСО-А лично без использования канала связи с оформлением соответствующей записи в журнале по форме (Приложение №15).

18.9.2 Администратор безопасности должен хранить дистрибутив на съемном носителе. Должны быть приняты меры по надежному хранению ключевых дистрибутивов (№152-ФЗ, №242-ФЗ) и другой ключевой информации, размещенной на съемных носителях. При отсутствии условий хранения дистрибутивов на рабочих местах они должны быть уничтожены с соответствующей отметкой в журнале учета СКЗИ Абонента.

18.10 Резервные наборы персональных ключей.

18.10.1Резервные наборы формируются Администратором Оператора ВЗСПДЗ РСО-А и передаются Администратору безопасности Абонента ВЗСПДЗ РСО-А, вместе с дистрибутивом справочно-ключевой информации.

18.10.2Резервные наборы должны храниться на съемных носителях. Запрещается хранение наборов на мобильных компьютерах и на компонентах ВЗСПДЗ РСО-А в помещениях, в которые могут иметь доступ посторонние лица.

18.10.3При отсутствии условий для хранения данных наборов они должны быть уничтожены вместе с дистрибутивами для первичной инициализации.

18.11 Личные ключи пользователя.

18.11.1Личные ключи могут передаваться пользователю вместе с дистрибутивом для первичной инициализации или переноситься на ключевой носитель в процессе первичной инициализации.

19 Режим работы ВЗСПДЗ РСО-А и технические мероприятия

19.1 Технические мероприятия по обслуживанию компонентов ВЗСПДЗ организуются Оператором и/или (при необходимости) Администратором безопасности соответствующего Абонента.

19.2 Плановые работы проводятся по графику, разрабатываемому Оператором.

19.3 К плановым работам относятся:

– реконфигурирование компонентов ВЗСПДЗ РСО-А;

– установка (переустановка) ПО, в том числе ОС на АП Абонента;

– техническое обслуживание компонентов ВЗСПДЗ РСО-А.

– другие виды работ, необходимость проведения которых определяется Оператором.

19.4 Оператор ВЗСПДЗ РСО-А осуществляет периодический контроль работоспособности компонентов ВЗСПДЗ РСО-А.

19.4.1 Контроль может осуществляться как непосредственно на проверяемом компоненте, так и удаленно. Контрольная проверка осуществляется в следующих случаях:

– при вводе компонента ВЗСПДЗ РСО-А в эксплуатацию;

– при смене лица, ответственного за эксплуатацию;

– периодически, по графику, разрабатываемому Оператором.

– внеплановая проверка при возникновении подозрений о компрометации данных, попытке изменения подключения ЛВС или подключения стороннего оборудования доступа к защищённой сети.

19.5 При обнаружении фактов сбоев в работе ПО или нарушения правил эксплуатации Администратор безопасности ВЗСПДЗ РСО-А обязан принять меры для устранения выявленных нарушений, уведомив об этом Оператора.

19.6 В случае возникновения нештатных ситуаций Администраторы безопасности, с привлечением Администратора Оператора, обязаны восстановить работоспособность обслуживаемых ими сегментов ВЗСПДЗ РСО-А в максимально сжатые сроки.

20 Порядок проверки выполнения требований Положения

20.1 Оператор имеет право проводить проверки компонентов ВЗСПДЗ РСО-А Абонентов с целью выявления фактов несоблюдения требований Положения. Оператор имеет право проводить внеплановую удалённую проверку с использованием программных комплексов.

20.2 Оператор имеет право не информировать Абонентов о своем визите с целью проведения проверки.

20.3 По результатам проведенной проверки Оператор составляет Протокол в котором указываются выявленные нарушения.

20.4 В случае выявления невыполнения требований настоящего Положения Оператор предоставляет Абоненту время на устранение несоответствий сроком равным от 1 до 30 (тридцать) дней с момента составления Протокола проверки в зависимости от выявленных нарушений.

21 Порядок обращения при инцидентах в работе ВЗСПДЗ РСО-А

21.1. При возникновении проблем при работе ВЗСПДЗ РСО-А, Пользователи обращаются к Администратору безопасности Абонента, который проводит первичную диагностику. Администратор безопасности Абонента формирует заявку в техническую поддержку ВЗСПДЗ РСО-А и направляет ее по электронной почте на адрес miac@minzdrav-rso.ru.

21.2. Для уточнения состояния заявок и получения дополнительной информации работает телефон горячей линии 40-49-57 в период с 9 до 17 часов.

21.3. При подаче заявки Администратор безопасности должен указать:

- наименование МО;
- ФИО пользователя;
- телефон, адрес электронной почты контактного лица;
- цель обращения/описание неисправности, а также мероприятия, проведенные при самостоятельной диагностике.

21.4. По факту регистрации заявки ответным письмом сообщается регистрационный номер, который в дальнейшем используется им при общении с сотрудниками технической поддержки в ходе разрешения заявки. В случае нарушения требований данного Положения, послужившего причиной сбоя функционирования ВЗСПДЗ РСО-А или НСД к информации, разглашения, компрометации, уничтожения, несанкционированного изменения информации, циркулирующей в ВЗСПДЗ РСО-А, все категории пользователей несут ответственность в соответствии с действующим законодательством.

22. Заключительные положения

В случае нарушения требований данного Положения, послужившего причиной сбоя функционирования ВЗСПДЗ РСО-А или НСД к информации, разглашения, компрометации, уничтожения, несанкционированного изменения информации, циркулирующей в ВЗСПДЗ РСО-А, все категории пользователей несут ответственность в соответствии с действующим законодательством.

Приложение 1

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

ЗАЯВЛЕНИЕ

на подключение к ведомственной защищенной сети передачи данных
в сфере охраны здоровья

Наименование учреждения _____ _____

ИНН _____

**В случае подключения нескольких средств СКЗИ – указывать информацию обо всех*

СКЗИ №____

Адрес подключения	*Указывается фактический адрес установки СКЗИ (Город, почтовый адрес)....*
Наименование СКЗИ	*Указывается СКЗИ, с использованием, которого будет производиться подключение к защищенной сети (Пример: ViPNet Client 3.2;АПКШ Континент ipc-100).*
Направления связи для организации защищённого обмена информацией	*Указывается общий перечень Абонентов, с которыми необходима организация защищённого обмен (Пример: ГБУЗ РСО-А «Кировская ЦРБ»). Защищенный обмен с ГБУЗ РМИАЦ РСО-А осуществляется по умолчанию.*
ФИО пользователя	*Заполняется только при подключении с использованием СКЗИ ViPNetClient; Континент АП.*
Структурное подразделение	
Электронная почта	
Телефон	

(*Все поля заполняются максимально полно. Фамилия, имя, отчество впечатываются полностью без сокращений в **ИМЕНИТЕЛЬНОМ ПАДЕЖЕ**, все поля заполняются исключительно в печатном виде, путем редактирования на компьютере с последующем распечатыванием на принтере. Заполнение «от руки» **НЕДОПУСТИМО**.)

Ответственным пользователем за эксплуатацию СКЗИ Ведомственной защищенной сети передачи данных в сфере охраны здоровья в

_____ назначен _____

(наименование учреждения) (ФИО)

На основании приказа «О назначении ответственных лиц» от «____» _____ 20__г. №_____ уполномоченн(ым)ому лиц(ам)у предоставлены полномочия по эксплуатацию СКЗИ.

Поставщик СКЗИ **«Наименование организации-поставщика СКЗИ»**

Администратор безопасности _____ /_____ /

Подпись

Руководитель учреждения _____ /_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 2

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

(наименование организации)

ПРИКАЗ

«____» _____ _____ года № ___

О назначении администратора безопасности и лиц его замещающих

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием средств криптографической защиты информации (СКЗИ) информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну

П Р И К А З Ы В А Ю:

1. Назначить администратором безопасности и возложить функции по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности СКЗИ:

_____
(Ф.И.О., должность, подразделение, реквизиты и контакты юридического лица либо ИП при наличии договора сопровождения,e-mail, телефон)

_____
(Ф.И.О., должность, подразделение, реквизиты и контакты юридического лица либо ИП при наличии договора сопровождения,e-mail, телефон)

2. Администратору безопасности провести инструктаж и обучение Пользователя(-ей) СКЗИ и ознакомить под роспись с правилами эксплуатации СКЗИ.

3. Администратор безопасности обязан:

- контролировать соблюдение Пользователями конфиденциальности при обращении со сведениями, которые им доверены или стали известны в процессе выполнения должностных обязанностей, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых компонентов Ведомственной защищенной сети передачи данных в сфере охраны здоровья (далее – ВЗСПДЗ РСО-А) и ключевых документов к ним;
- проводить ознакомление Пользователей с правилами работы и требованиями безопасности компонентов ВЗСПДЗ РСО-А;
- осуществлять хранение эксплуатационной и технической документации, ключевых документов, носителей информации ограниченного распространения относящихся к компонентам ВЗСПДЗ РСО-А, в соответствии с требованиями действующего законодательства;
- соблюдать правила эксплуатации СКЗИ;
- принимать меры по препятствованию несанкционированного доступа к компонентам ВЗСПДЗ РСО-А со стороны посторонних лиц;
- принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи

криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

4. Назначенный в п. 1 настоящего приказа сотрудник несет персональную ответственность за:

- обеспечение конфиденциальности информации, ставшей ему известной в процессе выполнения должностных обязанностей;
- сохранность ключевой информации;
- соблюдение правил эксплуатации программных и программно-аппаратных средств ViPNet, Континент.

5. Настоящий приказ вступает в силу со дня его подписания.

6. Контроль за выполнением настоящего Приказа оставляю за _____.

Руководитель учреждения _____ /_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 3

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

(наименование организации)

ПРИКАЗ

«____» _____ _____ года № ___

О назначении лиц, допускаемых к самостоятельной работе
со средствами криптографической защиты информации

Для осуществления мероприятий по организации доступа к сервисам и информационным системам Ведомственной защищенной сети передачи данных в сфере охраны здоровья с использованием средств криптографической защиты информации

П Р И К А З Ы В А Ю:

1. К самостоятельной работе с СКЗИ допустить следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность

2. В своей работе Пользователям ВЗСПДЗ РСО-А руководствоваться Положением о ВЗСПДЗ РСО-Алания и нормативными правовыми актами РФ в области защиты информации.

3. Настоящий приказ вступает в силу со дня его подписания.

4. Контроль за выполнением настоящего Приказа возложить на _____.

Руководитель учреждения _____ /_____/
Подпись

«____» _____ 201_ г

М.П.

Приложение 4

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

ДОВЕРЕННОСТЬ № _____
на получение средств криптографической защиты информации и электронно-цифровой подписи

Дата выдачи:

_____
(дата прописью)

_____,
(наименование организации)

в лице _____,
(должность и ФИО руководителя - полностью)

действующего на основании _____

настоящей доверенностью уполномочивает _____

_____
(должность и ФИО – полностью)

(паспорт серии _____ № _____, выдан «___» _____ _____ года
_____) представлять интересы
(кем выдан)

_____и получить
(наименование организации)

средства криптографической защиты информации (СКЗИ), а так же дистрибутивы ключей для первичного запуска прикладной программы сети ViPNet или Континент и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Ответственным в _____
(наименование организации)

за работу с СКЗИ назначен _____
(Ф.И.О., занимаемая должность)

_____.

Доверенность действительна до «___» _____ 20___ года и дана без права передоверия.

Подпись лица, получившего доверенность _____.
(подпись)

Руководитель _____ (_____)
(подпись) *(инициалы и фамилия)*

М.П.

«____»_____20___г.

Приложение 5

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

Требования по выделению адресного пространства Абонента при подключении программно-аппаратного комплекса к Ведомственной защищенной сети передачи данных в сфере охраны здоровья (ВЗСПДЗ РСО-А)

Для подключения ПАК ViPNet на территории Абонент должен:

1. Обеспечить подключение к одному из каналов передачи данных:

- IP/MPLS-сеть;
- Сеть Интернет (любые провайдеры, доступные в регионе).

2. При подключении через сеть Интернет обеспечение доступности внешнего интерфейса криптошлюза (IP внеш.) из сети Интернет одним из следующих способов:

2.1. Обеспечение NAT-трансляции частного IP-адреса в публичный IP-адрес (трафик по протоколу UDP, порт 55777).

2.2. Выделение для интерфейса публичного IP-адреса.

3. Обеспечить маршрутизацию в локальной сети Абонента таким образом, чтобы трафик с адресов серверов или автоматизированных рабочих мест Абонента, отправляемый на серверы ведомственной защищенной сети передачи данных в сфере здравоохранения, направлялся на внутренний интерфейс криптомаршрутизатора.

4. Для организации подключения ПАК ViPNet либо АПКШ «Континент» ВЗСПДЗ РСО-А необходимо обеспечить выделение следующих IP адресов:

п/п	IP адрес/маска	Назначение
1	IP внеш./маска	IP-адрес и маска сети внешнего интерфейса ПАК ViPNet либо АПКШ Континент. Может быть как из частного, так и из публичного адресного пространства.
2	IPgw внеш.	Адрес шлюза по умолчанию в сети, в которую включается внешний интерфейс ПАК ViPNet .
3	IPfw (NAT)	Публичный Интернет адрес NAT-трансляции, через который осуществляется доступ к внешнему интерфейсу ПАК ViPNet либо АПКШ «Континент» Указывается в случае использования частного адреса на внешнем интерфейсе ПАК ViPNet при подключении через сеть Интернет. При подключении ПАК ViPNet либо АПКШ «Континент» в сеть Интернет напрямую IP fw совпадает с IP внеш./маска.
4	IP внут./маска	Адрес и маска сети внутреннего (-их) интерфейса(-ов) ПАК ViPNet . IP внеш. и IP внут. обязательно должны принадлежать разным подсетям.
5	IPgw внут.	Адрес шлюза для доступа к внутренним ресурсам организации. Указывается в случае нахождения ресурсов организации и внутреннего интерфейса ПАК ViPNet либо АПКШ «Континент» разных сетях.
6	IP тунн.	Адрес сервера или АРМ (диапазон адресов), которые будут взаимодействовать с серверами ВЗСПДЗ РСО-А.

Приложение 6

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

Отзыв заявления о присоединении к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья государственного бюджетного учреждения здравоохранения Республики Северная Осетия Алания «Медицинский информационно-аналитический центр»

_____

(наименованиеОрганизации, включая организационно-правовую форму)

_____

в лице

(должность,ФИО)

_____

_____

действующегонаосновании_____

Адрес места нахождения: _____

(указывается адрес места нахождения юридического лица)

_____

Адрес для переписки:_____

(указываются почтовый адрес юридического лица и адрес электронной почты)

_____

Государственный регистрационный номер записи о создании юридического лица (ОГРН):_____

Идентификационный номер налогоплательщика (ИНН) _____

Сотрудник, уполномоченный по вопросам присоединения к Положению_____

_____

(указываются наименование должности, ФИО, номера телефонов, адрес электронной почты)

просит аннулировать заявление о присоединении к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья государственного бюджетного учреждения здравоохранения Республики Северная Осетия Алания «Медицинский информационно-аналитический центр» (далее – ГБУЗ РСО-А «МИАЦ»)зарегистрированное в реестре пользователей ВЗСПДЗ РСО-А регистрационный номер №_____ от «____»_____20____г.

и исключить_____

(наименование Организации, включая организационно-правовую форму)

_____

из реестра пользователей ВЗСПДЗ РСО-А.

_____ _____ _____

(должность руководителя организации) (подпись) (ФИО)

М.П.

(заполняется уполномоченным сотрудником ГБУЗ РСО-А «МИАЦ»)

Заявление о присоединении к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья ГБУЗ РСО-А «МИАЦ»регистрационный номер №_____ от «____»_____20____г. аннулировано.

Дата исключения из реестра пользователей ВЗСПДЗ РСО-А ГБУЗ РСО-А «МИАЦ» «_____»_____.

Директор ГБУЗ РСО-А «МИАЦ» _____ _____

Приложение 7

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

Заявление о присоединении к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья государственного бюджетного учреждения здравоохранения Республики Северная Осетия-Алания «Медицинский информационно-аналитический центр»

_____
(наименование Организации, включая организационно-правовую форму)

_____

в лице_____
(должность, ФИО)

_____

действующегонаосновании_____
в соответствии со статьей 428 Гражданского кодекса Российской Федерации полностью и безусловно присоединяется к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья государственного бюджетного учреждения здравоохранения Республики Северная Осетия Алания «Медицинский информационно-аналитический центр» (далее – ГБУЗ РСО-А «МИАЦ»), условия которого определены ГБУЗ РСО-А «МИАЦ».

Адрес места нахождения: _____
(указывается адрес места нахождения юридического лица)

_____

Адрес для переписки: _____
(указываются почтовый адрес юридического лица и адрес электронной почты)

_____

Государственный регистрационный номер записи о создании юридического лица (ОГРН):_____
Идентификационный номер налогоплательщика (ИНН) _____
Сотрудник, уполномоченный по вопросам присоединения к Положению_____

_____
(указываются наименование должности, ФИО, номера телефонов, адрес электронной почты)

С Положением о ведомственной защищенной сети передачи данных в сфере охраны здоровья ГБУЗ РСО-А «МИАЦ» и приложениями к нему ознакомлен (-а)и обязуюсь соблюдать все требования указанного документа.

_____ _____ _____
(должность руководителя организации) (подпись) (ФИО)

М.П.

(заполняется уполномоченным сотрудником ГБУЗ РСО-А «МИАЦ»)

Заявление о присоединении к Положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья ГБУЗ РСО-А«МИАЦ» зарегистрировано в реестре пользователей ВЗСПДЗРСО-А.
Регистрационный номер №_____ от «____»_____20____г.

Директор ГБУЗ РСО-А«МИАЦ» _____ _____

Приложение 8

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

СОГЛАШЕНИЕ №_____
об установлении межсетевого взаимодействия

г. Владикавказ «__» _____201_ г.

Государственное бюджетное учреждение здравоохранения Республики Северная Осетия Алания «Медицинский информационно-аналитический центр», в лице директора_____, действующего на основании Устава, в дальнейшем именуемое ГБУЗ РСО-А «МИАЦ», с одной стороны, и_____
(наименование Организации, включая организационно-правовую форму)

_____

в лице _____.
(должность, ФИО)

действующего на основании _____,
именуемое в дальнейшем «_____»,
(сокращенное наименование Организации)

с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1 Предмет соглашения

1.1 Стороны договорились об установлении межсетевого взаимодействия и доверия между сетевыми узлами ViPNet сети ГБУЗ РСО-А «МИАЦ» (далее – ViPNet *№ 3223*) и сетевыми узлами ViPNet сети «_____» (далее – ViPNet №_____). Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между разрешенными сетевыми узлами ViPNet сетей Сторон.

1.2 Отношения между Сторонами регулируются следующими нормативными документами:

• Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

• Методическими рекомендациями Министерства здравоохранения Российской Федерации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения;

• 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».

1.3 Взаимодействие Сторон осуществляется на безвозмездной основе.

2 Права и обязанности сторон

2.1 При организации межсетевого взаимодействия ГБУЗ РСО-А «МИАЦ» принимает на себя следующие права и обязанности:

2.1.1 Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet *№ 3223* в границах своей зоны ответственности.

2.1.2 Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet *№* ___ согласно разделу 3.

2.2 При организации межсетевого взаимодействия *«_____»* принимает на себя следующие права и обязанности:

2.2.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов ViPNet *№* ____ в границах своей зоны ответственности.

2.2.2 Обеспечивает организацию взаимосвязи с сетевыми узлами ViPNet *№* _____ согласно разделу 3.

2.3 Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью (далее – ЦУС) ViPNet-сетей. Экспортированные данные импортируются в ЦУС соответствующей сети (Приложение 1).

3 Организация межсетевого взаимодействия

3.1 Ответственными лицами Сторон для организации межсетевого взаимодействия являются администраторы ЦУС. На начальном этапе организуется межсетевое взаимодействие только между абонентскими пунктами (далее – АП) администраторов ЦУС Сторон через шлюзовые ViPNet-Координаторы в соответствии с технической документацией на программное обеспечение (далее – ПО) ViPNet-администратор. Этим обеспечивается установление доверия между ViPNet-сетями Сторон.

3.2 По завершении процедуры организации межсетевого взаимодействия между ViPNet *№3223* и ViPNet *№* _____, подписывается Протокол установления межсетевого взаимодействия (Приложение 2).

3.3 При необходимости установления дополнительных связей между сетевыми узлами Сторон администраторы ЦУС устанавливают данное взаимодействие руководствуясь технической документацией на ПО ViPNet-Администратор на основании заявки, форма которой указана в Приложении 3 к настоящему Соглашению. Экземпляр правильно оформленной заявки может быть передан администратору ЦУС стороной-инициатором в электронном виде.

3.4 После согласования обновленного списка сетевых узлов администраторы ViPNet-сетей обмениваются соответствующими экспортами и выполняют соответствующие действия для установления связи между такими узлами.

3.5 Список подключенных сетевых узлов между абонентами ViPNet *№ 3223* и ViPNet *№* _____ отображается в Матрице связи (Приложение 4).

3.6 Матрица связи дополняется (изменяется) по мере изменения данных, указанных в списке подключенных сетевых узлов.

4 Проведение профилактических мероприятий

4.1 Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности. Стороны обязаны осуществлять не чаще 1 раза в месяц при соблюдении следующих условий:

• срок проведения профилактических мероприятий не должен превышать 1 дня;

• профилактические мероприятия должны проводиться в пределах первых пяти календарных дней месяца;

• о сроках проведения профилактических мероприятий другая Сторона должна быть оповещена заблаговременно, не позднее, чем за 7 дней до дня проведения профилактических мероприятий.

4.2 В случае возникновения необходимости проведения технических работ, следствием которых может быть временное прекращение работоспособности программных и программного аппаратных комплексов ViPNet Сторона-инициатор должна уведомить другую Сторону любым удобным способом.

5 Ответственность сторон

5.1 Стороны несут ответственность за обеспечение безопасности информации, передаваемой по средствам программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности согласно законодательству Российской Федерации.

5.2 Стороны не несут ответственность за содержание информации, передаваемой с применением технологии ViPNet.

6 Сроки действия соглашения

6.1 Настоящее Соглашение вступает в силу с момента его подписания, и действует в течение одного года.

6.2 Действие настоящего Соглашения автоматически продлевается на следующий календарный год, если ни одна из Сторон не заявит о его прекращении не позднее, чем за месяц до истечения строка действия настоящего Соглашения.

6.3 Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию Сторон, либо в одностороннем порядке с предупреждением другой Стороны за два месяца до расторжения Соглашения.

7 Форс-мажор

7.1 При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2 Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую Сторону в течение трех рабочих дней с предоставлением документов компетентных органов, подтверждающих наличие данных обстоятельств.

7.3 Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

8 Дополнительные условия

8.1 В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

8.2 При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между ViPNet *№ 3223* и ViPNet № _____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

8.3 Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

8.4 В случае изменения наименования, адреса места нахождения или других реквизитов одной из Сторон Сторона письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

8.5 Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8.6 К настоящему Соглашению прилагаются к качестве неотъемлемой части следующие приложения:

8.6.1 Приложение 1. Состав защищенных сетей и границы зоны ответственности сторон.

8.6.2 Приложение 2. Форма протокола установления межсетевого взаимодействия.

8.6.3 Приложение 3. Заявка на добавление абонентских пунктов в экспорт сети ViPNet *№ 3223.*

8.6.4 Приложение 4. Матрица связей между сетевыми узлами ViPNet *№ 3223* и ViPNet *№* _____

2 Адреса и реквизиты сторон

ГБУЗ
«РМИАЦ» МЗ РСО-А

Юридический адрес:

Фактическое местонахождение:

ИНН,
КПП
р/с

Директор

_____**Майрамукаев А.А.**
МП

_____/_____/
МП

Приложение 8

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

СОГЛАШЕНИЕ №_____
об установлении межсетевого взаимодействия

г. Владикавказ «__» _____201_ г.

Государственное бюджетное учреждение здравоохранения Республики Северная Осетия Алания«Медицинский информационно-аналитический центр», в лице директора_____, действующего на основании Устава, в дальнейшем именуемое ГБУЗ РСО-А «МИАЦ», с одной стороны, и_____
(наименование Организации, включая организационно-правовую форму)

_____

в лице _____,
(должность, ФИО)

действующего на основании _____,
именуемое в дальнейшем «_____»,
(сокращенное наименование Организации)

с другой стороны, совместно именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1 Предмет соглашения

1.1 Стороны договорились об установлении межсетевого взаимодействия и доверия между сетевыми узлами АПКШ «Континент» сети ГБУЗ РСО-А «МИАЦ» и сетевыми узлами АПКШ «Континент» сети «_____». Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между разрешенными сетевыми узлами АПКШ «Континент» сетей Сторон.

1.2 Отношения между Сторонами регулируются следующими нормативными документами:

• Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

• Методическими рекомендациями Министерства здравоохранения Российской Федерации медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках единой государственной информационной системы в сфере здравоохранения;

• 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».

1.3 Взаимодействие Сторон осуществляется на безвозмездной основе.

2 Права и обязанности сторон

2.1 При организации межсетевого взаимодействия ГБУЗ РСО-А «МИАЦ» принимает на себя следующие права и обязанности:

2.1.1 Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов АПКШ «Континент» в границах своей зоны ответственности.

2.1.2 Обеспечивает организацию взаимосвязи с сетевыми узлами АПКШ «Континент» № ___ согласно разделу 3.

2.2 При организации межсетевого взаимодействия «_____» принимает на себя следующие права и обязанности:

2.2.1. Обеспечивает поддержание в работоспособном состоянии программных и программно-аппаратных комплексов АПКШ «Континент» № ____ в границах своей зоны ответственности.

2.2.2 Обеспечивает организацию взаимосвязи с сетевыми узлами АПКШ «Континент» № _____ согласно разделу 3.

2.3 Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью (далее – ЦУС) АПКШ «Континент» - сетей. Экспортированные данные импортируются в ЦУС соответствующей сети (Приложение 1).

3 Организация межсетевого взаимодействия

3.1 Ответственными лицами Сторон для организации межсетевого взаимодействия являются администраторы ЦУС. На начальном этапе организуется межсетевое взаимодействие только между абонентскими пунктами (далее – АП) администраторов ЦУС Сторон через шлюзовые АПКШ «Континент» - Координаторы в соответствии с технической документацией на программное обеспечение (далее – ПО) АПКШ «Континент» администратор. Этим обеспечивается установление доверия между АПКШ «Континент» - сетями Сторон.

3.2 По завершении процедуры организации межсетевого взаимодействия между АПКШ "Континент"- МИАЦ и АПКШ «Континент» № _____, подписывается Протокол установления межсетевого взаимодействия (Приложение 2).

3.3 При необходимости установления дополнительных связей между сетевыми узлами Сторон администраторы ЦУС устанавливают данное взаимодействие руководствуясь технической документацией на ПО АПКШ «Континент» - Администратор на основании заявки, форма которой указана в Приложении 3 к настоящему Соглашению. Экземпляр правильно оформленной заявки может быть передан администратору ЦУС стороной-инициатором в электронном виде.

3.4 После согласования обновленного списка сетевых узлов администраторы АПКШ «Континент» - сетей обмениваются соответствующими экспортами и выполняют соответствующие действия для установления связи между такими узлами.

3.5 Список подключенных сетевых узлов между абонентами АПКШ «Континент» - МИАЦ и АПКШ «Континент» № _____ отображается в Матрице связи (Приложение 4).

3.6 Матрица связи дополняется (изменяется) по мере изменения данных, указанных в списке подключенных сетевых узлов.

4 Проведение профилактических мероприятий

4.1 Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов АПКШ «Континент» в границах своей зоны ответственности Стороны обязаны осуществлять не чаще 1 раза в месяц при соблюдении следующих условий:

• срок проведения профилактических мероприятий не должен превышать 1 дня;

• профилактические мероприятия должны проводиться в пределах первых пяти календарных дней месяца;

• о сроках проведения профилактических мероприятий другая Сторона должна быть оповещена заблаговременно, не позднее, чем за 7 дней до дня проведения профилактических мероприятий.

4.2 В случае возникновения необходимости проведения технических работ, следствием которых может быть временное прекращение работоспособности программных и программного аппаратных комплексов АПКШ «Континент» Сторона-инициатор должна уведомить другую Сторону любым удобным способом.

5 Ответственность сторон

5.1 Стороны несут ответственность за обеспечение безопасности информации, передаваемой по средствам программных и программно-аппаратных комплексов АПКШ «Континент» в границах своей зоны ответственности согласно законодательству Российской Федерации.

5.2 Стороны не несут ответственность за содержание информации, передаваемой с применением технологии АПКШ «Континент»

6 Сроки действия соглашения

6.1 Настоящее Соглашение вступает в силу с момента его подписания, и действует в течение одного года.

6.2 Действие настоящего Соглашения автоматически продлевается на следующий календарный год, если ни одна из Сторон не заявит о его прекращении не позднее, чем за месяц до истечения строка действия настоящего Соглашения.

6.3 Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию Сторон, либо в одностороннем порядке с предупреждением другой Стороны за два месяца до расторжения Соглашения.

7 Форс-мажор

7.1 При возникновении обстоятельств, которые делают полностью или частично невозможным выполнение настоящего Соглашения одной из Сторон, таких как стихийные бедствия, военные действия и другие обстоятельства непреодолимой силы, не зависящие от сторон, сроки исполнения обязательств продлеваются на время, в течение которого действуют эти обстоятельства.

7.2 Сторона, подвергшаяся действию форс-мажорных обстоятельств, обязуется уведомить письменно другую Сторону в течение трех рабочих дней с предоставлением документов компетентных органов, подтверждающих наличие данных обстоятельств.

7.3 Если обстоятельства непреодолимой силы действуют более одного месяца, Соглашение может быть досрочно расторгнуто в одностороннем порядке, путем заключения дополнительного соглашения.

8 Дополнительные условия

8.1 В случае возникновения споров и разногласий Стороны прилагают все усилия, чтобы устранить их путём переговоров.

8.2 При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между АПКШ «Континент» МИАЦ и АПКШ «Континент» № _____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

8.3 Любые изменения и дополнения к Соглашению действительны, если они совершены в письменной форме и подписаны надлежащим образом уполномоченными на то представителями Сторон.

8.4 В случае изменения наименования, адреса места нахождения или других реквизитов одной из Сторон Сторона письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

8.5 Настоящее Соглашение составлено в двух экземплярах, имеющих одинаковую юридическую силу, по одному для каждой из Сторон.

8.6 К настоящему Соглашению прилагаются к качестве неотъемлемой части следующие приложения:

8.6.1 Приложение 1. Состав защищенных сетей и границы зоны ответственности сторон.

8.6.2 Приложение 2. Форма протокола установления межсетевого взаимодействия.

8.6.3 Приложение 3. Заявка на добавление абонентских пунктов в экспорт сети АПКШ «Континент» МИАЦ.

8.6.4 Приложение 4. Матрица связей между сетевыми узлами АПКШ «Континент» МИАЦ и АПКШ «Континент» № _____.

3 Адреса и реквизиты сторон

ГБУЗ
«РМИАЦ» МЗ РСО-А

Юридический адрес:

Фактическое местонахождение:

ИНН,
КПП
р/с

Директор

_____**Майрамукаев А.А.**
МП

_____/_____/
МП

Приложение 9

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

АКТ
вывода СКЗИ из эксплуатации

«___» _____ 20___ г.

Комиссия в составе: председателя комиссии _____,

членов комиссии _____

и администратора безопасности СКЗИ _____

составила акт о том, что (наименование СКЗИ) установленный в

_____

по адресу_____

в помещении №_____ выведен в эксплуатацию «___» _____ 20___ г.

Состав (наименование СКЗИ):

Системный блок № _____

Программный комплекс:

(наименование СКЗИ) версия _____ сборка _____

Uin:
Id:
Mac:

Председатель комиссии:

_____	_____	_____
Должность	Ф.И.О.	Подпись

Члены комиссии:

_____	_____	_____
Должность	Ф.И.О.	Подпись
_____	_____	_____
Должность	Ф.И.О.	Подпись

Приложение 10

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

ЗАЯВЛЕНИЕ

на регистрацию маршрутизатора и присвоение данных для организации доступа к ведомственной защищенной сети передачи данных
в сфере охраны здоровья

Полное и сокращенное наименование учреждения _____
_____

Юридический и физический адрес учреждения _____
_____

Производитель, модель и серийный номер маршрутизатора_____
_____

Информация об основном провайдере_____
_____

Статический сетевой IP адрес основного провайдера_____
_____

Информация о резервном провайдере _____
_____

Статический сетевой IP адрес резервного провайдера _____
_____

Количество АРМ и периферийного сетевого абонентского оборудования_____
_____

Количество активного сетевого оборудования абонента _____
_____

Администратор безопасности _____/_____/

Руководитель учреждения _____
/_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 11

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

ЗАЯВЛЕНИЕ

На проверку корректности настройки для организации доступа к ведомственной защищенной сети передачи данных
в сфере охраны здоровья

Номер технологической площадки_____

_____

Тип оборудования_____

_____

Физическое расположение (здание, литер, этаж/межэтаж , № кабинета)_____

_____

Сетевой IP адрес_____

_____

Имя коммутатора (в соответствии с принятой системой именования оборудования, АРМ и периферии – Приложение №14)_____

_____

Логин и пароль с полным доступом к настройкам оборудования_____

_____

SNMP версия и community_____

_____

SNMP логин и пароль (в случае использования авторизации)_____

_____

Администратор безопасности _____ /_____ /

Руководитель учреждения _____
/_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 12

к положению о ведомственной защищенной сети передачи данных в сфере охраны здоровья

ЗАЯВЛЕНИЕ

На регистрацию АРМ абонента для организации доступа к ведомственной защищенной сети передачи данных в сфере охраны здоровья

Номер технологической площадки_____

_____

Имя АРМ (в соответствии с принятой системой именования оборудования, АРМ и периферии – Приложение №14)_____

_____

Физическое расположение (здание, литер, этаж/межэтаж , № кабинета)_____

_____

Физический адрес сетевой карты АРМ (при наличии более 1 сетевой карты адреса для каждой, с указанием порта подключенного к защищённой сети, второй интерфейс должен быть отключен программно и опечатан)_____

_____

Имя коммутатора и номер порта к которому подключается АРМ_____

_____

Версия операционной системы (Обязательно наличие лицензионной ОС с поддержкой подключения к Microsoft Active Directory)_____

_____

Версия антивирусного программного обеспечения совместимая с центром управления антивирусным ПО Kaspersky Security Center с действующей лицензией (при наличии программного обеспечения для данной операционной системы)_____

_____

Иное программное обеспечение, установленное на АРМ_____

_____

Администратор безопасности _____/_____/

Руководитель учреждения _____

/_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 13

к положению о ведомственной
защищенной сети передачи данных
в сфере охраны здоровья

ЗАЯВЛЕНИЕ

На подключение пользователя абонента к ведомственной защищенной сети передачи данных в сфере охраны здоровья

Название организации абонента_____
_____

ФИО пользователя_____
_____

Учётная запись пользователя в домене_____
_____

Подразделение и должность пользователя_____
_____

Наименование информационного ресурса_____
_____

Протоколы и порты (при необходимости)_____
_____

Права доступа (при необходимости)_____
_____

Причина предоставления/прекращения доступа_____
_____

Дата начала действия_____
_____

Предоставить или прекратить доступ_____
_____

Администратор безопасности _____/_____/

Руководитель учреждения _____
/_____/

Подпись

«____» _____ 201_ г

М.П.

Приложение 14

Именование объектов.

1. Именование технологических площадок

Имя технологических площадок состоит из английских букв TP и трёхзначного порядкового номера. Нумерация осуществляется сотрудниками поддержки доменной инфраструктуры.

Пример: TP001

2. Именование роутеров и коммутаторов и иного сетевого оборудования

Сетевое имя состоит из имени технологической площадки, обозначения типа оборудования и двузначного порядкового номера. Для обозначения роутеров используется английская буква R, коммутаторов — SW. Остальное оборудование именуется аналогично.

Пример: TP001R01, TP001SW01

3. Именование компьютеров

Имя компьютера состоит из обозначения типа компьютера указываемого английской буквой (W — рабочая станция, T — терминальный клиент, N — ноутбук), трёхзначного номера технологической площадки, номера здания на площадке (если одно, то указывается 0), номера этажа (одна цифра) и двузначного порядкового номера. Каждый тип компьютера имеет свою нумерацию начинающуюся с «01». При этом расположение компьютера указывается в его описании в оснастке AD «Пользователи и компьютеры». При создании

Пример: W0010301, T0010101, N0010201

4. Именование принтеров

Имя принтера состоит из английской буквы P, трёхзначного номера технологической площадки, номера здания на площадке (если одно, то указывается 0), номера этажа (одна цифра) и двузначного порядкового номера. При этом расположение принтера указывается в его описании на сервере печати.

Пример: P0010301

5. Именование пользователей

Имя входа пользователя состоит из имени, знака точка и фамилии в транслитерации согласно прилагаемой таблице. При заведении пользователя в домене указывается на русском языке его имя, фамилия и инициалы в виде одной буквы имени, знака точка,

одной буквы фамилии и знака точка. После создания пользователя, в свойствах его учётной записи вносятся данные о его местоположении (комната — номер кабинета), контактном номере телефона (в формате «+7(XXX)XXX-XX-XX»), должности, организации (берётся из описания технологической площадки пользователя), отделе, адресе (берётся из описания технологической площадки пользователя), почтовом индексе (берётся из описания технологической площадки пользователя).

Если необходимо создать групповую учётную запись, то именование производится следующим образом — английская буква U, трёхзначного номера технической площадки, подразделение, специализация. При необходимости нескольких учётных записей по данному критерию, добавляется номер кабинета. Если в данном кабинете одновременно установленны несколько рабочих мест, то для них используется одна учётная запись.

Пример: U001PriemUrolog, U001PriemKardiolog102

Транслитерация при именовании объектов

Русский алфавит	Транслит
А, а	a
Б, б	b
В, в	v
Г, г	g
Д, д	d
Е, е	e,ye(после мягкого знака)
Ё, ё	e,ye(после мягкого знака)
Ж, ж	zh
З, з	zh
И, и	i
Й, й	y
К, к	k
Л, л	l
М, м	m
Н, н	n
О, о	o
П, п	p
Р, р	r
С, с	s
Т, т	t
У, у	u
Ф, ф	f
Х, х	kh
Ц, ц	tc
Ч, ч	ch
Ш, ш	sh
Щ, щ	shch
Ъ, ъ	-
Ы, ы	y
Ь, ь	-
Э, э	e
Ю, ю	yu
Я, я	ya

Приложение 15
к положению о ведомственной защищенной сети
передачи данных в сфере охраны здоровья

ЖУРНАЛ
поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов

№	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	ФИО пользователя СКЗИ	Дата и расписка в получении
	1	2	3	4	5	6	7
1							___.___.201__ № _____

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, произведших подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены СКЗИ	Дата изъятия (уничтожения)	Ф.И.О. сотрудников органа криптографической защиты, пользователя СКЗИ, производивших изъятие (уничтожение)	Номер акта или расписка об уничтожении	
8	9	10	11	12	13	14
			___.___.201__			

Приложение 16

к положению о ведомственной защищенной сети
передачи данных в сфере охраны здоровья

ТЕХНИЧЕСКИЙ (АППАРАТНЫЙ)

ЖУРНАЛ

№ п/п	Дата	Тип и регистрационные номера	Запись об обслуживании криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10