КОМИТЕТ ЗДРАВООХРАНЕНИЯ
ВОЛГОГРАДСКОЙ ОБЛАСТИ
(ОБЛЗДРАВ)

ПРИКАЗ

25 июля 2022 г. № 151н

Волгоград

Об утверждении порядка подключения к государственной информационной системе Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области" и организации межсетевого взаимодействия с защищенной сетью государственной информационной системы Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области"

В соответствии с постановлением Губернатора Волгоградской области от 29 декабря 2012 г. № 1447 "О государственной информационной системе Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области"

п р и к а з ы в а ю:

1. Утвердить прилагаемый порядок подключения к государственной информационной системе Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области" и организации межсетевого взаимодействия с защищенной сетью государственной информационной системы Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области" (далее – Порядок).

2. Рекомендовать использование Порядка юридическими лицами независимо от организационно-правовой формы или индивидуальными предпринимателями, осуществляющими на территории Волгоградской области в качестве уставного вида деятельности медицинскую деятельность на основании лицензии, выданной в порядке, установленном законодательством Российской Федерации о лицензировании отдельных видов деятельности.

3. Контроль исполнения приказа возложить на заместителя председателя комитета здравоохранения Волгоградской области Алимова Н.Н.

Временно осуществляющий полномочия
председателя комитета здравоохранения
Волгоградской области И.А. Карасева

КОМИТЕТ ЗДРАВООХРАНЕНИЯ ВОЛГОГРАДСКОЙ ОБЛАСТИ
канцелярия
Российская Федерация

УТВЕРЖДЕН

приказом комитета
здравоохранения
Волгоградской области
от 25 июля 2022 г. № 151н

Порядок
подключения к государственной информационной системе Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области" и организации межсетевого взаимодействия с защищенной сетью государственной информационной системы Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области"

1. Список терминов и сокращений

VPN	Виртуальная частная сеть (Virtual Private Network - VPN); VPN: территориально распределенная корпоративная логическая сеть, создаваемая на базе уже существующих сетей (локальных корпоративных сетевых структур, сетей связи общего пользования, сети Интернет, сетей связи операторов связи), имеющая сходный с основной сетью набор услуг и отличающаяся высоким уровнем защиты данных согласно ГОСТ Р 53729-2009. Национальный стандарт Российской Федерации. Качество услуги "Предоставление виртуальной частной сети (VPN)". Показатели качества" (утвержден и введен в действие Приказом Ростехрегулирования от 15.12.2009 № 1193-ст)
ViPNet-сеть	VPN-сеть, построенная с использованием технологий ViPNet
АРМ	Автоматизированное рабочее место
Администратор ViPNet-сети	Назначенный приказом сотрудник Участника / Оператора, осуществляющий администрирование ViPNet-сети, принадлежащей данному Участнику / Оператору
Администратор информационной безопасности	Назначенный приказом сотрудник Участника, отвечающий за информационную безопасность Организации
ГИС "РИСЗ ВО"	Государственная информационная система Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области"
Защищенная ViPNet-сеть	ViPNet-сеть № 13582 (КСЗ) ГИС "РИСЗ ВО"
Поставщик информации в ГИС	Юридические лица независимо от организационно-правовой формы или индивидуальные предприниматели,

"РИСЗ ВО"	осуществляющие на территории Волгоградской области в качестве уставного вида деятельности медицинскую деятельность на основании лицензии, выданной в порядке, установленном законодательством Российской Федерации о лицензировании отдельных видов деятельности
Значимый объект критической информационной инфраструктуры	Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры
ИСММК	Индивидуальный симметричный межсетевой мастер-ключ
Компрометация ключей	Событие, определенное владельцем квалифицированного сертификата (сертификата) как ознакомление неуполномоченным лицом (неуполномоченными лицами) с его ключом электронной подписи, хищение, утеря или несанкционированное копирование ключевого носителя, другие причины появления у владельца квалифицированного сертификата (сертификата) сомнений в сохранении тайны ключа электронной подписи
Сетевой узел	Персональный компьютер с установленным ПКЗИ ViPNet Client 4.x / ПАК "ViPNet Coordinator HW"
Объект критической информационной инфраструктуры	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры
Оператор	Государственное бюджетное учреждение здравоохранения "Волгоградский областной медицинский информационно-аналитический центр", Волгоград
Пользователь	Назначенный приказом Участника / Оператора сотрудник, использующий для выполнения своих служебных обязанностей сервисы и информационные системы ViPNet-сети Участника / Оператора
Сторонняя ViPNet-сеть	ViPNet-сеть Пользователя или Участника
Участник	Организация, подключенная к Защищенной ViPNet-сети или осуществляющая межсетевое взаимодействие с Защищенной ViPNet-сетью
Центр управления сетью (далее – ЦУС)	Аппаратные или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети

2. Общие положения.

2.1. Настоящий Порядок определяет организацию подключения к Защищенной ViPNet-сети, организацию межсетевого взаимодействия

с Защищенной ViPNet-сетью, а также порядок работы в Защищенной ViPNet-сети.

2.2. Порядок разработан в соответствии с:

– Постановлением Правительства РФ от 09.02.2022 № 140 "О единой государственной информационной системе в сфере здравоохранения" (вместе с "Положением о единой государственной информационной системе в сфере здравоохранения");

– Приказом Министерства здравоохранения РФ от 24.12.2018 № 911н "Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций";

– Федеральным законом от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации";

– Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";

– Федеральным законом от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации";

– Приказом ФСТЭК России от 25.12.2017 № 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации";

– Приказом ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

– Приказом ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";

– Приказом ФАПСИ № 152 от 13.06.2001 "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";

– Постановлением Губернатора Волгоградской области от 29.12.2012 № 1447 "О государственной информационной системе Волгоградской области "Региональная информационная система в сфере здравоохранения Волгоградской области";

– иными нормативными актами, регулирующими отношения в области защиты информации.

2.3. При наличии у Заявителя значимых объектов критической информационной инфраструктуры, которые будут взаимодействовать с информационными системами Защищенной ViPNet-сети, порядок организации межсетевого взаимодействия определяется пунктом 3.2 раздела 3 настоящего Порядка.

3. Организация взаимодействия Заявителя с Защищенной ViPNet-сетью.

Настоящий Порядок определяет организацию взаимодействия Заявителя с Защищенной ViPNet-сетью путем:

– подключения с использованием программных или программно-аппаратных комплексов ViPNet-сети №13582;

– организации межсетевого взаимодействия ViPNet-сети Заявителя с Защищенной ViPNet-сетью.

3.1. Подключение с использованием программных или программно-аппаратных комплексов ViPNet-сети №13582.

Организация подключения Заявителя к Защищённой ViPNet-сети с использованием программных или программно-аппаратных комплексов ViPNet-сети №13582 включает в себя следующие стадии:

– предварительная стадия;

– заявительная стадия;

– стадия рассмотрения заявления;

– формирование и передача ключевой информации для доступа к информационным системам.

3.1.1. Предварительная стадия.

Заявителю, желающему подключиться к Защищённой ViPNet-сети, до момента подачи заявления в адрес Оператора о намерении подключиться к Защищённой ViPNet-сети необходимо:

– если количество АРМ, подключаемых к Защищённой ViPNet-сети, не превышает 5 шт., самостоятельно приобрести ПКЗИ ViPNet Client 4.x;

– если количество АРМ, подключаемых к Защищённой ViPNet-сети, от 5 до 10 включительно, то рекомендуется самостоятельно приобрести ПАК "ViPNet Coordinator HW 100";

– если количество АРМ, подключаемых к Защищённой ViPNet-сети, превышает 10, то рекомендуется самостоятельно приобрести ПАК "ViPNet Coordinator HW 1000";

– при оформлении договорных отношений по приобретению ПКЗИ ViPNet Client 4.x и/или ПАК ViPNet Coordinator HW Участник указывает номер Защищённой ViPNet-сети для подключения – **13582**;

– проведение мероприятий по аттестации объекта информатизации на соответствие требованиям по безопасности информации, предъявляемым к государственным информационным системам не ниже класса К2.

3.1.2. Заявительная стадия.

Заявитель направляет в адрес Оператора заявление о намерении подключиться к Защищённой ViPNet-сети (Приложение 1 к настоящему Порядку).

Заявление должно содержать:

– контакты лиц, ответственных за организацию подключения Участника (ФИО, должность, контактный телефон, электронная почта);

– перечень Участников, с которыми необходима организация защищенного обмена;

– перечень информационных ресурсов Защищённой ViPNet-сети, к которым необходимо организовать доступ;

– копию аттестата соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам класса защищенности не ниже К2.

3.1.3. Стадия рассмотрения заявления.

Оператор в течение 5-ти рабочих дней со дня получения заявления о намерении подключиться к Защищённой ViPNet-сети проводит оценку оснований для подключения к Защищённой ViPNet-сети, технической возможности, организации направлений связи и доступа к информационным системам и принимает решение о подключении заявителя к Защищённой ViPNet-сети или об отказе в подключении к Защищённой ViPNet-сети.

Решение о подключении к Защищённой ViPNet-сети направляется в письменной форме в адрес Заявителя в течение 3-х рабочих дней со дня принятия указанного решения.

Оператор имеет право отказать Участнику в подключении к Защищённой ViPNet-сети, объяснив причину отказа. Решение об отказе в подключении к Защищённой ViPNet-сети направляется в письменной форме в адрес Участника в течение 3-х рабочих дней со дня принятия указанного решения.

Участник после получения решения от Оператора о подключении заключает соглашение об информационном взаимодействии с Оператором.

3.1.4. Формирование и передача ключевой информации для доступа к информационным системам.

Участник после заключения Соглашения об информационном взаимодействии формирует и направляет в адрес Оператора заявку на подключение по форме согласно приложению 2 к настоящему Порядку.

В случае использования ПКЗИ ViPNet Client 4.x в заявке указываются:

– условное наименование сетевого узла;

– ФИО пользователя;

– наименование информационного ресурса, к которому необходимо предоставить доступ.

В случае использования ПАК "ViPNet Coordinator HW" в заявке указываются:

– статический IP-адрес для "внешнего" интерфейса ПАК "ViPNet Coordinator HW", подключенного к сети Интернет;

– статический IP-адрес для "внутреннего" интерфейса ПАК "ViPNet Coordinator HW", подключенного к локальной сети Заявителя;

– IP-адреса туннелируемых сетевых узлов;

– наименование информационного ресурса, к которому необходимо предоставить доступ.

В течение 3-х рабочих дней со дня получения от Участника заявки на подключение Оператор:

– проводит регистрацию сетевых узлов в Защищенной ViPNet-сети;

– формирует дистрибутивы ключей для сетевых узлов;

– организовывает доступ к обозначенным информационным ресурсам;

– по завершению обозначенных работ уведомляет об этом Заявителя.

Участник для получения дистрибутива ключей и пароля доступа к нему должен направить к Оператору представителя с носителем информации и доверенностью на получение дистрибутива ключей по форме согласно приложению 3 к настоящему Порядку.

Факт выдачи дистрибутива ключей заносится в Журнал учета выдачи ключевых документов.

После получения дистрибутива ключей Заявитель считается Участником.

3.2. Межсетевое взаимодействие ViPNet-сети Участника с Защищенной ViPNet-сетью.

Организация межсетевого взаимодействия ViPNet-сети Заявителя с Защищённой ViPNet-сети включает в себя следующие стадии:

– подача заявки;

– рассмотрение заявки;

– настройка межсетевого взаимодействия.

3.2.1. Подача заявки.

Для организации межсетевого взаимодействия с Защищённой ViPNet-сетью Заявитель формирует и направляет в адрес Оператора заявку в виде информационного письма по форме согласно приложению 4 к настоящему Порядку, в котором указывает (прилагает копии документов):

– контакты лиц, ответственных за организацию межсетевого взаимодействия (ФИО, должность, контактный телефон, электронная почта);

– номер подключаемой VipNet-сети Заявителя;

– класс используемого для организации межсетевого взаимодействия СКЗИ VipNet (КС3);

– используемая версия программного комплекса VipNet Administrator Сторонней VipNet-сети;

– копия аттестата соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам класса защищенности не ниже К2, выданный на сегмент Сторонней ViPNet-сети;

– наименование сетевых узлов, подключённые к ViPNet-сети Заявителя, ФИО пользователей сетевых узлов;

– наименование ПАК ViPNet Coordinator HW, выбранный в качестве

шлюзового координатора ViPNet-сети Заявителя;

– наименование информационных ресурсов, к которым необходим доступ.

3.2.2. Рассмотрение заявки.

Оператор в течение 5-ти рабочих дней со дня получения заявления проводит предварительный анализ заявки, включая оценку технической возможности для организации межсетевого взаимодействия. В случае принятия решения о технической возможности организации межсетевого взаимодействия Оператор уведомляет в письменной форме Организацию Сторонней сети, инициирующий заявку, о принятии такого решения, назначает дату передачи ИСММК на АРМ Администратора Сторонней ViPNet-сети для установления межсетевого взаимодействия.

Оператор имеет право отказать в организации межсетевого взаимодействия. Причины для отказа могут быть следующими:

– сведения, перечень которых определен в п. 3.2.1, предоставлены не в полном объеме, с указанием недостающих сведений;

– класс используемого для организации межсетевого взаимодействия СКЗИ Сторонней сети отличный от класса КС3;

– копия аттестата соответствия требованиям безопасности информации на сегмент сторонней ViPNet-сети не предоставлен и (или) не соответствует предъявленным требованиям безопасности информации к государственным информационным системам класса защищенности не ниже К2.

В случае принятия решения об организации межсетевого взаимодействия Заявитель и Оператор заключают соглашение об установлении межсетевого взаимодействия, руководствуясь технической документацией по организации межсетевого взаимодействия сетей VipNet.

3.2.3. Настройка межсетевого взаимодействия.

После заключения соглашения об установлении межсетевого взаимодействия Оператор и Заявитель осуществляют формирование и передачу ИСММК:

– Оператор осуществляет формирование ИСММК для Заявителя;

– Заявителю по защищенному каналу передаются экспортные файлы, в состав которых входят экспортные справочники, ИСММК, пароль на ИСММК, а также форма подтверждения, любым способом, исключающим несанкционированный доступ (далее - НСД) к пересылаемой информации;

– после получения экспортных файлов Заявитель осуществляет настройку межсетевого канала;

– после получения ответного экспорта от Заявителя по защищенному каналу Оператор осуществляет установку ответного экспорта из ViPNet-сети Заявителя.

После выполнения всех действий Оператор и Заявитель осуществляют проверку межсетевого взаимодействия.

По итогам организованного межсетевого взаимодействия обе стороны подписывают в 2-х экземплярах Протокол установления межсетевого взаимодействия по форме согласно приложению 5 к настоящему Порядку и обмениваются подписанными экземплярами документа.

4. Разрешение конфликтных ситуаций.

Возникновение конфликтных ситуаций межсетевого взаимодействия может быть связано с формированием, доставкой, получением, подтверждением получения или компрометацией электронных документов и / или получением доступа к информационным системам Защищенной ViPNet-сети.

Разрешение конфликтных ситуаций осуществляется путём взаимодействия Администраторов Участников межсетевого взаимодействия.

В случае выявления нарушений в части защиты персональных данных разрешение конфликта производится в соответствии с законодательством Российской Федерации.

5. Ответственность.

За ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, Участники Защищенной ViPNet-сети №13582 несут ответственность в пределах, определенных действующим законодательством Российской Федерации.

Приложение 1
к Порядку

Директору ГБУЗ "Волгоградский областной медицинский информационно-аналитический центр", Волгоград

О подключении к Защищенной сети ViPNet № 13582 ГИС ВО "РИСЗ ВО"

Прошу подключить _____ к Защищенной сети ViPNet № 13582 ГИС ВО "РИСЗ ВО" для обмена информацией.

Предполагаемое число подключаемых абонентских пунктов – _____

Перечень информационных ресурсов (подсистем ГИС ВО "РИСЗ ВО"), к которым необходим доступ:

_____

Лицо, ответственное за подключение, и контактный телефон:

_____

Копия аттестата соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам, прилагается.

Руководитель организации
(или индивидуальный предприниматель) _____/ФИО/

М.П. (при наличии)

Приложение 2
к Порядку

ЗАЯВКА
на подключение к защищенной сети ГИС "РИСЗ ВО"
№ 13582

1. Полное наименование организации (ФИО индивидуального предпринимателя)
2. Сокращенное наименование организации
3. Юридический адрес организации (адрес места жительства (регистрации) индивидуального предпринимателя)
4. Наименование сетевой узел / ФИО Пользователя: Клиент № 1, Пользователь: _____ Клиент № 2, Пользователь: _____
5. IP-адрес внешнего и внутреннего интерфейса ПАК ViPNet Coordinator HW (в случае использования): Внешний IP- адрес: 94.5.10.12, Маска: 255.255.255.0 Шлюз по умолчанию: 94.5.10.254 Внутренний IP- адрес: 172.21.10.10
6. IP-адреса туннелируемых сетевых узлов (случае использования ПАК ViPNet Coordinator HW): Туннель: 172.21.10.12 / 172.21.10.13, 172.21.10.14 / 172.21.10.12 – 172.21.10.14
7. Взаимодействие с сетевыми узлами для организации защищенного обмена информацией (если требуется): Участник Защищенной сети передачи данных 1 Участник Защищенной сети передачи данных 2
8. Перечень информационных ресурсов (подсистем РИСЗ) Защищенной сети передачи данных, к которым необходим доступ (если требуется) МИС "Инфоклиника" ИС "ВКС"

Руководитель организации

(или индивидуальный предприниматель) _____/ФИО/

М.П. (при наличии)

Приложение 3
к Порядку

Доверенность
на получение дистрибутива ключей к Защищенной сети ViPNet № 13582

(наименование населенного пункта) «___»_____20___г.

Наименование организации в лице руководителя _____, действующего на основании Устава (Положения), или индивидуальный предприниматель (ФИО) _____уполномочивает:

_____, паспорт серия _____ номер _____, выданный _____ «___» _____ 20__г. получить в ГБУ "Центр информационных технологий" Волгоградской области дистрибутив ключей для первичного запуска ПКЗИ ViPNet Client 4.x / ПАК ViPNet Coordinator HW сети ViPNet № 13582.

Настоящая доверенность действительна до «___»_____20___г.

Подпись лица, получившего доверенность _____

Руководитель организации

(или индивидуальный предприниматель) _____/ФИО/

М.П. (при наличии)

Приложение 4
к Порядку

Директору ГБУЗ "Волгоградский областной
медицинский информационно-аналитический
центр", Волгоград

О межсетевом взаимодействии
с Защищенной сетью ViPNet № 13582
ГИС ВО "РИСЗ ВО"

С целью межведомственного защищенного информационного взаимодействия прошу Вас организовать межсетевое взаимодействие VipNet сети №_____ наименование организации _____ (ФИО индивидуального предпринимателя) с Защищенной сетью ViPNet № 13582 ГИС «РИСЗ».

1. Лицо, ответственное за организацию межсетевого взаимодействия (ФИО, должность, контактный телефон, электронная почта)_____

2. Номер подключаемой VipNet-сети _____

3. Класс используемого СКЗИ ViPNet _____

4. Используемая версия программного комплекса VipNet Administrator _____

5. Наименование сетевого узла / ФИО Пользователя:

Клиент №1, Пользователь: _____

Клиент №2, Пользователь: _____

6. Наименование шлюзового координатора:

ViPNet Coordinator HW №1.

7. Перечень информационных ресурсов Защищенной сети передачи данных, к которым необходим доступ (если требуется): МИС "Инфоклиника", ИС "ВКС"

Копия аттестата соответствия требованиям безопасности информации, предъявляемым к государственным информационным системам, выданный на сегмент VipNet сети №_____ наименование организации, прилагается.

Руководитель организации

(или индивидуальный предприниматель) _____/ФИО/

М.П. (при наличии)

Приложение 5
к Порядку

ПРОТОКОЛ
установления межсетевого взаимодействия
«___»_____20___г.

1. Межсетевое взаимодействие устанавливается между сетями:

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

2. Целью установления межсетевого взаимодействия является межведомственное защищенное информационное взаимодействие ViPNet сетей указанных организаций.

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№_____		
№_____		

4. Передача начального и ответного экспорта между сетями №_____ и №_____ осуществлялась через специалиста, уполномоченного на данные действия.

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

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

в сети №_____ - "_____"

в сети №_____ - "_____"

7. Смена межсетевых ключей, изменение состава Участников межсетевого взаимодействия, производится после предварительного согласования в письменном виде, о чем администраторы защищенных сетей уведомляют друг друга с указанием производимых изменений.

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

Руководитель организации владельца сети ViPNet № _____

_____
(ФИО)

_____
(подпись)

«___»_____20___г.

М.П. . (при наличии)

Руководитель организации владельца сети ViPNet № _____

_____
(ФИО)

_____
(подпись)

«___»_____20___г.

М.П. . (при наличии)