федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный медицинский университет»
Министерства здравоохранения Российской Федерации (ФГБОУ ВО СамГМУ Минздрава России)

ПРИКАЗ

28.12.2024 № 259

Самара

О вводе в действие регламентирующей документации

В целях регулирования порядка работы с информационно-телекоммуникационной системой ФГБОУ ВО СамГМУ Минздрава России, составляющей совокупность средств вычислительной техники, информационных систем, автоматизированных систем и оборудованием, обеспечивающим их взаимодействие в информационно-телекоммуникационных сетях организации

ПРИКАЗЫВАЮ:

1. Утвердить Регламент установки и обновления программного обеспечения в ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 1, к настоящему приказу;
2. Утвердить Регламент резервного копирования в ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 2, к настоящему приказу;
3. Утвердить Регламент удалённого доступа к сети ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 3, к настоящему приказу;
4. Утвердить Регламент подключения к защищённой сети передачи данных VipNet 14369 ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 4, к настоящему приказу;
5. Утвердить Инструкцию по использованию персонального компьютера и ресурсов сети ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 5, к настоящему приказу;
6. Утвердить Регламент подключения, сопровождения и технического обслуживания средств вычислительной техники и телекоммуникационного оборудования в ифнормационно-телекоммуникационной системе ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 6, к настоящему

приказу;

7. Утвердить Порядок проведения работ по обслуживанию информационных систем в ФГБОУ ВО СамГМУ Минздрава России согласно Приложению № 7, к настоящему приказу;

8. Контроль за исполнением настоящего приказа возложить на директора Института цифрового развития Одобеску С.В.

Ректор **А.В. Колсанов**

Приложение №4 к приказу
от «28» 12 2024 г. № 259

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ»
Министерства здравоохранения Российской Федерации

РЕГЛАМЕНТ № 17917

подключения к защищенной сети передачи данных ViPNet №14369
ФГБОУ ВО СамГМУ Минздрава России

Самара 2024

1. Термины и определения

АРМ	- автоматизированное рабочее место
ЗСПД	- защищенная сеть передачи данных;
ИС	- информационная система;
ПАК	- программно-аппаратный комплекс;
ПО	- программное обеспечение;
СКЗИ	- средство криптографической защиты информации;
ЦУС	- центр управления сетью;
ViPNet Administrator	- программное обеспечение для администрирования и управления сетью ViPNet;
ViPNet Client	- программный комплекс, выполняющий на рабочем месте пользователя функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы, а также криптопровайдера для прикладных программ, использующих
ViPNet Coordinator	- сетевой узел сети - программно-аппаратный комплекс ViPNet Coordinator, размещаемый на границах сетей или сегментов сети и выполняющий в рамках сети ViPNet серверные функции, маршрутизацию трафика и служебной информации;
ViPNet Сеть	- сеть, организованная с помощью ПО ViPNet и представляющая собой совокупность защищенных сетевых узлов сети ViPNet. Сеть ViPNet имеет свою адресацию, позволяющую организовать обмен информацией между ее узлами. Каждая сеть ViPNet имеет свой уникальный номер (идентификатор);
Внешняя сеть	- сеть, имеющая другое адресное пространство по отношению к внутренней сети. Как правило, этот термин используется для обозначения глобальной сети Интернет.
	Внешняя сеть по отношению к рассматриваемой внутренней сети является физически и(или) логически самостоятельной и имеет свое адресное пространство, которое не должно пересекаться с адресным пространством рассматриваемой внутренней сети;
Внутренняя сеть	- локальная сеть, подлежащая защите.
	Для организации внутренней сети используются IP - адреса из пространства адресов, *не применяемых в Интернете;*
Дистрибутив ключей	- файл с расширением. dst, создаваемый для каждого сетевого узла ViPNet и устанавливаемый на узел. В файл помещены адресные справочники, ключевая информация и файл лицензии, необходимые для обеспечения первичного запуска и
Защищенный узел сети	- оборудование сети с установленным ПО ViPNet с функцией шифрования трафика на сетевом уровне;
Коммуникационное ядро	- комплекс сетевых устройств, обеспечивающих резервирование каналов и высокоскоростную передачу данных
Открытый узел сети	- оборудование сети, с которым обмен информацией происходит в незашифрованном виде;

УИБ	Управление информационной безопасности, Института цифрового развития, СамГМУ
Туннелирование	- шифрование трафика открытых узлов сети при передаче через сеть общего пользования;
Файл экспорта	файл, содержащий данные об экспортированных сетевых узлах, коллективах и пользователях, данные об сервере маршрутизаторе, через который будет осуществляться взаимодействие с другой

2. Назначение документа

Настоящий документ разработан с целью определения порядка подключения внешних организаций (далее - Заявители) к ЗСПД Федерального государственного бюджетного образовательное учреждение высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации (далее - СамГМУ) для организации защищенного взаимодействия.

3. Общие сведения о защищенной виртуальной сети

ЗСПД организована на базе сертифицированных по требованиям безопасности информации СКЗИ, обеспечивающих создание защищенной доверенной среды передачи данных, транспортной средой для которой может являться как сеть Интернет, так и любой коммутируемый канал на базе протокола IP.

ЗСПД обеспечивает выполнение требований безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну,

ЦУС ЗСПД и его коммуникационное ядро размещены в СамГМУ и реализованы с использованием соответственно программного комплекса ViPNet Administrator и программно-аппаратных комплексов ViPNet Coordinator HW.

Одной из функций ЦУС ЗСПД является выдача дистрибутивов ключей, изготовленных организацией, лицензиатом ФСБ России на основании государственного контракта.

Дистрибутивы ключей используются для средств ViPNet, которые включаются в логическую структуру ЗСПД, то есть могут рассматриваться как узлы ЗСПД, но при этом в состав ЗСПД не входят (например, по признаку собственника средства ViPNet).

В случае наличия у заявителя собственной защищенной сети ViPNet и обязательного в этом случае установленного в сети средства управления сетью (программного комплекса ViPNet Administrator), средствами ЦУС изготавливается файл экспорта сети ЗСПД и сети ViPNet заявителя.

При этом изготовление дистрибутива ключей для узлов сети ViPNet заявителя осуществляется самим заявителем без обращения к услугам ЦУС ЗСПД.

4. Объекты подключения к защищенной сети

В качестве объектов сети заявителя, подключаемых к ЗСПД, рассматриваются:

- ПАК ViPNet Coordinator HW (100/1000/2000);
- АРМ с установленным ПО ViPNet Client.

Указанные средства создают шифрованный канал передачи данных и по терминологии сетей ViPNet называются защищенными узлами сети. При организации взаимодействия открытых узлов сети заявителя и информационных ресурсов, размещенных в ЗСПД, применяется механизм туннелирования трафика.

В режиме туннелирования передаваемые данные остаются незащищенными только на участке от АРМ заявителя до его ViPNet Coordinator HW, в дальнейшем все данные подвергаются шифрованию.

Количество туннелируемых узлов определяется конфигурацией оборудования ViPNet Coordinator HW.

5. Порядок подключения к защищенной сети

Подключение к ЗСПД осуществляется на основе поступивших в СамГМУ заявок (письменных обращений).

Заявка на подключение к ЗСПД, подписанная руководителем заявителя, направляется в адрес УИБ СамГМУ (адрес 443099, г. Самара, ул. Чапаевская, 89 каб. 103, эл.почта cib@samsmu.ru). В зависимости от типа подключения к ЗСПД к заявке необходимо приложить данные согласно п.5.1. по форме, указанной в Приложении 1 или п.5.2., по форме, указанной в Приложении 2.

После рассмотрения заявка направляется администратору ЗСПД, который организует выдачу заявителю дистрибутива ключей, файлов экспорта, а также их хранение.

5.1. В заявке указываются следующие сведения:

- полное наименование заявителя (органа/организации/учреждения);
- подключаемые к сети защищенные узлы;
- фамилия, имя, отчество сотрудников (пользователей) заявителя, подключаемых к сети ЗСПД;
- почтовый адрес установки узла ЗСПД;
- фамилия, имя, отчество лица, ответственного за организацию подключения со стороны заявителя, с указанием должности, контактного телефона, электронной почты;

Дополнительные данные о наличии у заявителя регистрационных файлов подключаемых защищенных узлов могут запрашиваться у заявителя администратором ЗСПД в рабочем порядке.

5.2. При наличии у заявителя собственной защищенной сети ViPNet между СамГМУ и заявителем заключается Соглашение о межсетевом взаимодействии VipNet-сетей (далее - Соглашение), по форме, указанной в Приложении 2. Подписанное в двух экземплярах соглашение вместе с заявкой на подключение к ЗСПД направляется в СамГМУ.

Если для исполнения своих служебных обязанностей участнику ЗСПД СамГМУ необходим доступ к информационным ресурсам, расположенным в другой ЗСПД, участник, предварительно согласовав с СамГМУ возможность организации межсетевого взаимодействия, самостоятельно направляет для подписания владельцу ЗСПД проект соглашения по форме, указанной в Приложении 2. Далее, подписанные владельцем ЗСПД экземпляры соглашения направляются в СамГМУ. Допускается подписание соглашения по форме владельца ЗСПД.

5.3. Настройка и подключение средств ViPNet заявителя к ЗСПД возможна при наличии файлов *.dst (файла экспорта) и сведений по IP-адресации взаимодействующих информационных ресурсов, а именно:

- ip-адреса внешних интерфейсов ViPNet Coordinator HW в сети Интернет;
- ip-адреса внешних интерфейсов шлюза межсетевого взаимодействия;
- ip-адрес сервера информационного ресурса в сети, с которым организуется взаимодействие;
- ip-адреса узлов локальной сети заявителя (например, АРМ), для которых должен быть организован шифрованный трафик путем установки ПО ViPNet Client на данные узлы (частные IP-адреса из адресного пространства сети);
- ip-адреса АРМ в пространстве адресов локальной сети заявителя, для которых должен быть разрешен режим туннелирования в сеть ЗСПД (частные ip-адреса из адресного пространства сети).

При модернизации ЗСПД, настройки и порядок подключения к ЗСПД уточняются ответственным лицом заявителя.

Приложение 1 к регламенту подключения

к защищенной сети ViPNet СамГМУ

Директору института цифрового развития СамГМУ
С.В. Одобеску

ЗАЯВКА

на подключение к защищенным ресурсам сети ViPNet №14369

наименование организации

в лице _____

должность (не ниже заместителя руководителя), Ф.И.О.

подтверждает готовность рабочего места* к подключению сетевого узла к защищенным ресурсам сети ViPNet № 14369 и просит произвести его подключение:

1.	Имя сетевого узла ViPNet Client *(заполняется при подключении администратором сети)*	
2.	Полное наименование заявителя (организации, подключаемой к защищенной сети)	
3.	ФИО сотрудника(ов), рабочее место которого(ых) подключается к защищенной сети с указанием должности, контактного телефона, электронной почты	
4.	Почтовый адрес установки узла защищенной сети (район, город (поселение), улица, дом, кабинет)	
5.	ФИО сотрудника, ответственного за организацию подключения со стороны заявителя, с указанием должности, контактного телефона, электронной почты	
	Обеспечить доступ к следующим защищенным ресурсам сети ViPNet № 14369: (например, СЭД «Тандем» и (или) ИС «1С:Бухгалтерия» и (или) др.)	
6.	Наименование ресурса	

* - выполнение требований информационной безопасности (в том числе применение актуальных лицензионных версий отечественного антивирусного программного обеспечения *(включенного в Единый реестр российских программ для электронных вычислительных машин и баз данных)* с ежедневным обновлением баз вирусных сигнатур, организация парольной защиты, контролируемый доступ к рабочему месту, назначение ответственных за информационную безопасность лиц и др.).

_____ / /

должность подпись Ф.И.О

Приложение 2 к регламенту
подключения к защищенной
сети ViPNet СамГМУ

СОГЛАШЕНИЕ №
о межсетевом взаимодействии ViPNet-сетей

г. Самара «____» _____ 202 __г.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации (ФГБОУ ВО СамГМУ Минздрава России), в лице _____, действующего на основании _____, и _____, с одной стороны, и _____, в лице _____, действующего на основании _____ , 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 СамГМУ области (далее - ViPNet №14369) и сетевыми узлами ViPNet-сети (далее - ViPNet № _____). Межсетевое взаимодействие должно обеспечивать создание защищенной, доверенной среды передачи информации ограниченного доступа между разрешенными сетевыми узлами, входящими в сети ViPNet 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»;
- Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
- Приказом ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- Приказом ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»;
- Приказом ФСБ РФ от 27 декабря 2011 г. № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи»
- 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.

1.4. Состав защищенных сетей и границы зоны ответственности сторон указаны в Приложение №4 к настоящему Соглашению.

2. **Права и обязанности сторон.**

2.1. При организации межсетевого взаимодействия сторона ФГБОУ ВО СамГМУ Минздрава России принимает на себя следующие права и обязанности:

2.1.1. Осуществляет администрирование защищенной ViPNet-сети №14369.

2.1.2. В соответствии с законодательством Российской Федерации выполняет и соблюдает требования по обеспечению конфиденциальности информации, обрабатываемой в информационной системе, с использованием защищенной ViPNet- сети №14369.

2.1.3. Администрирует и обеспечивает работоспособность аппаратных, программных и телекоммуникационных средств, необходимых для штатного функционирования защищенной ViPNet-сети №14369.

2.1.4. Определяет работников (сотрудников), ответственных за взаимодействие в рамках настоящего Соглашения (далее - уполномоченные лица), и сообщает _____ об определении таких уполномоченных лиц с указанием их контактных данных, в соответствии с Приложением № 2 к настоящему Соглашению. Об изменении указанных сведений своевременно информирует.

2.2. При организации межсетевого взаимодействия сторона _____принимает на себя следующие права и обязанности:

2.2.1. Осуществляет администрирование защищенной ViPNet-сети №_____ .

2.2.2. В соответствии с законодательством Российской Федерации выполняет и соблюдает требования по обеспечению конфиденциальности информации, обрабатываемой в информационной системе , с использованием защищенной ViPNet-сети № _____.

2.2.3. Администрирует и обеспечивает работоспособность аппаратных, программных и телекоммуникационных средств, необходимых для штатного функционирования защищенной ViPNet-сети № .

2.2.4. Определяет работников (сотрудников), ответственных за взаимодействие в рамках настоящего Соглашения (далее - уполномоченные лица), и сообщает об определении таких уполномоченных лиц с указанием их контактных данных, в соответствии с Приложением № 2 к настоящему Соглашению. Об изменении указанных сведений своевременно информирует.

2.3. Стороны обеспечивают контроль за проведением процедуры обмена данными экспорта между центрами управления сетью ViPNet-сетей.

3. **Организация межсетевого взаимодействия.**

3.1. Стороны вносят данные в список ответственных лиц (Приложение № 2 к настоящему Соглашению).

3.2. Для организации межсетевого взаимодействия администраторы ViPNet-сетей Сторон производят формирование справочной и ключевой информации - формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой сети. Межсетевое взаимодействие осуществляется только с использованием актуальных сертифицированных версий программного обеспечения.

3.3. Указанные данные (начальный экспорт) в течение 2 (двух) рабочих дней после подписания Соглашения формируются администратором ViPNet-сети №14369 и направляются администратору ViPNet-сети №_____ .

3.4. Администратор ViPNet-сети № _____ , после обработки начального экспорта, формирует ответный экспорт для ViPNet-сети №14369 в соответствии с Приложением №1 к настоящему Соглашению.

3.5. Ответная информация (ответный экспорт) доверенным способом передается администратору ViPNet-сети №14369, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого взаимодействия между ViPNet-сетями Сторон, в дальнейшем обмен данными между ними производится в автоматическом режиме с предварительным уведомлением и фиксацией изменений в Журнале изменений по организации межсетевого взаимодействия ViPNet-сетей (Приложение № 3 к настоящему Соглашению), установленным порядком использования средств криптографической защиты информации.

3.6. Сформированная ключевая и справочная информация обрабатывается внутри защищенных ViPNet-сетей Сторон средствами своих центров управления сетью и самостоятельно направляется на свои абонентские пункты, участвующие в защищенном межсетевом взаимодействии.

3.7. После завершения процедуры организации межсетевого взаимодействия между сетями Сторон, подписывается протокол установления межсетевого взаимодействия по

форме Приложения № 1 к настоящему Соглашению.

3.8. Проведение профилактических мероприятий по поддержанию работоспособности программных и программно-аппаратных комплексов ViPNet в границах своей зоны ответственности Стороны обязаны осуществлять не чаще 1 (одного) раза в месяц, при этом срок проведения профилактических мероприятий не должен превышать 1 (один) день.

4. **Ответственность сторон.**

4.1. 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.

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

4.3. Стороны и иные лица, получившие доступ к защищаемой информации (информации ограниченного доступа, в том числе и персональным данным) в соответствии с настоящим Соглашением, обязаны не раскрывать третьим лицам и не распространять информацию ограниченного доступа (персональные данные) без письменного согласия субъекта персональных данных, если иное не предусмотрено Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Сроки действия соглашения.

5.1. Настоящее Соглашение вступает в силу с даты его подписания, и заключено на неопределенный срок.

5.2. Настоящее Соглашение может быть досрочно расторгнуто по обоюдному согласию Сторон, либо в одностороннем порядке при письменном уведомлении другой Стороны за 1 (один) месяц до даты предполагаемого расторжения Соглашения.

6. Форс-мажор.

6.1. 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.

6.2. 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.

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

7. Дополнительные условия.

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

7.2. При возникновении обстоятельств, которые не позволяют обеспечить межсетевое взаимодействие между ViPNet №14369 и ViPNet № _____ Стороны прилагают совместные усилия по устранению этих обстоятельств.

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

7.4. Сторона Соглашения, у которой изменились наименование, адрес места нахождения или иные реквизиты, письменно извещает об этом другую Сторону в течение трех рабочих дней со дня такого изменения.

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

7.6. К настоящему Соглашению прилагаются в качестве неотъемлемой части следующие приложения:

• Приложение 1 - Протокол установления межсетевого взаимодействия;

• Приложение 2 - Список уполномоченных лиц;

• Приложение 3 - Форма журнала изменений по организации межсетевого взаимодействия ViPNet-сетей;

• Приложение 4 - Состав защищенных сетей и границы зоны ответственности сторон.

8. Адреса и реквизиты сторон

Сторона 1	Сторона 2
Федеральное государственное бюджетное образовательное учреждение высшего образования "Самарский государственный медицинский университет» Министерства здравоохранения Российской Федерации (ФГБОУ ВО СамГМУ Минздрава России)	

Приложение № 3 к Соглашению
о межсетевом взаимодействии ViPNet-сетей
от «___»_____ 202__ г.

ФОРМА ЖУРНАЛА ИЗМЕНЕНИЙ ПО ОРГАНИЗАЦИИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ VIPNET-СЕТЕЙ

№ п/п	Наименование произведенного изменения в межсетевом взаимодействии	Дата изменения	Подпись специалиста, проводившего изменения

Пояснение по ведению Журнала изменений:

1. В журнал заносятся все события, которые относятся к организации защищенного информационного взаимодействия:

• установление межсетевого взаимодействия;
• выбор Координатора, выполняющего функции сервера-шлюза;
• формирование межсетевого мастер-ключа;
• плановая смена межсетевого мастер-ключа;
• смена ключей при их компрометации;
• модификация межсетевого взаимодействия (добавление или удаление сетевого узла, изменение состава туннелируемых ресурсов).

2. Каждая запись Журнала в обязательном порядке заверяется подписью специалиста (администратора СЗИ/СКЗИ), производившего изменения.

Приложение № 4 к Соглашению
о межсетевом взаимодействии ViPNet-сетей
от «___»_____ 202__ г.

СОСТАВ ЗАЩИЩЕННЫХ СЕТЕЙ И ГРАНИЦЫ ЗОНЫ ОТВЕТСТВЕННОСТИ СТОРОН

1 Состав защищенной сети ФГБОУ ВО СамГМУ Минздрава России.

1.1. Состав защищенной сети ФГБОУ ВО СамГМУ Минздрава России включает в себя:

ViPNet-Администратор - программный комплекс для настройки и управления защищенной сетью ФГБОУ ВО СамГМУ Минздрава России (ViPNet №14369);

Шлюзовой ViPNet-Координатор - сетевой узел, через который проходит весь межсетевой обмен со стороны ФГБОУ ВО СамГМУ Минздрава России (ViPNet № 14369).

Сетевые узлы - абонентские пункты и координаторы ViPNet № 14369.

2. Состав защищенной сети _____.

2.1. Состав защищенной сети _____ включает в себя:

ViPNet-Администратор - программный комплекс для настройки и управления защищенной сетью (ViPNet № _____);

Шлюзовой ViPNet-Координатор - сетевой узел, через который проходит весь межсетевой обмен со стороны (ViPNet № _____).

Сетевые узлы - абонентские пункты и координаторы ViPNet № _____.

3. Границы зоны ответственности Сторон.

3.1. Стороны Соглашения несут ответственность в случае нарушения работоспособности программных и программно-аппаратных комплексов ViPNet в границах принадлежащих им зон ответственности.

3.2. Стороны несут ответственность за контроль передачи данных через своего провайдера.

Стороны не несут ответственность за прекращение передачи данных, вызванных по вине провайдера.