Приложение №2 к Приказу №23
от «26» мая 2021 г.

УТВЕРЖДЕНО
Директор КУ НАО «НИАЦ»
_____Е.А. Ружников
«26» мая 2021 г

РЕГЛАМЕНТ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ УЧАСТНИКОВ ЗАЩИЩЕННОЙ СЕТИ «VIPNET» КАЗЕННОГО УЧРЕЖДЕНИЯ НЕНЕЦКОГО АВТОНОМНОГО ОКРУГА «НЕНЕЦКИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»

Нарьян-Мар
2021

1. Термины и определения

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

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

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

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

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

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

Локальный администратор - назначенный приказом сотрудник Участника, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному Участнику.

Координатор защищенной сети - сотрудник Оператора, осуществляющий общую политику администрирования всей Защищенной сети.

Владелец информационных систем - участник, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством.

Компрометация ключей - утрата доверия к тому, что используемые ключи обеспечивают безопасность информации.

Защищенная сеть - защищенная виртуальная сеть казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр», построенная по технологии ViPNet.

Оператор - казенное учреждение Ненецкого автономного округа «Ненецкий информационно-аналитический центр»,

Несанкционированный доступ - доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах путём изменения (повышения, фальсификации) своих прав доступа.

Претендент - организация, имеющая намерения подключиться к Защищенной сети.

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

ФАПСИ – Федеральное агентство правительственной связи и информации

ФЗ – Федеральный закон

ФСБ – Федеральная служба безопасности

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

2. Общие положения

Регламент информационного взаимодействия участников защищенной сети ViPNet казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр» (далее - Регламент) определяет механизмы, условия подключения к Защищенной сети, включая обязанности Участников защищенной сети, протоколы работы, процедуры взаимодействия сторон, принятые форматы документов и данных, основные организационно-технические мероприятия, необходимые для безопасной работы Защищенной сети.

Регламент разработан в соответствии с Федеральным законом от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации», 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 ФАПСИ от 13.06.2001 года № 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».

Регламент определяет и устанавливает:

- порядок организации и подключения Участников Защищенной сети (далее Участники) к защищенной виртуальной сети ViPNet №2440 Оператора (далее Защищенная сеть);
- порядок предоставления доступа к информационным системам Защищенной сети;
- порядок организации защищенного межсетевого взаимодействия;
- порядок действий при компрометации ключей;
- порядок разрешения конфликтных ситуаций.

3. Порядок организации подключения участников к защищенной сети

Подключение Участников к Защищенной сети включает в себя следующие стадии:

- заявительная стадия;
- стадия рассмотрения заявления;
- закупка программного обеспечения ViPNet [Клиент] Претендентом;
- формирование и передача ключевой информации;
- формирование и передача учетных записей для доступа к информационным системам.

Заявительная стадия.

Претендент, желающий подключиться к Защищенной сети, направляет в адрес Оператора заявление о намерении подключиться к Защищенной сети за подписью руководителя (Приложение №1).

В заявлении должна содержаться следующая информация:

- предполагаемое количество подключаемых Абонентских пунктов;
- перечень информационных ресурсов Защищенной сети, к которым необходимо организовать доступ;
- ФИО и контактный телефон лица, ответственного за подключение Претендента.

Стадия рассмотрения заявления.

Оператор в течение 3-х рабочих дней со дня получения заявления о намерении подключиться к Защищённой сети проводит оценку оснований для подключения Претендента к Защищённой сети, технической возможности организации направлений связи и доступа к информационным системам.

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

Оператор имеет право отказать Претенденту в организации доступа к информационным системам Защищенной сети, объяснив причину отказа.

Оператор уведомляет Претендента о принятии решения о подключении (отказе в подключении) к Защищённой сети, по указанными в заявлении контактным данным в течение 3-х рабочих дней со дня принятия указанного решения.

Закупка программного обеспечения ViPNet [Клиент] Претендентом.

В случае принятия положительного решения о подключении к Защищённой сети, Претендент самостоятельно приобретает программное обеспечение ViPNet [Клиент].

При оформлении договорных отношений по приобретению программного обеспечения ViPNet [Клиент] Претендент указывает номер Защищённой сети для подключения - 2440.

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

Оператор уведомляет Претендента о получении регистрационных файлов посредством электронной почты, указанной в заявление о намерении подключиться к Защищенной сети.

Формирование и передача ключевой информации.

Претендент, после получения информации о поступлении регистрационных файлов, оповещает Оператора.

Оператор в течение 2-х рабочих дней со дня оповещения от Претендента:

- производит регистрацию Абонентских пунктов в Центре управления сетью;
- организовывает связи между Абонентскими пунктами в соответствии с заявлением на подключение;
- организовывает доступ Абонентским пунктам к информационным ресурсам Защищенной сети в соответствии с заявлением на предоставление доступа к информационным ресурсам;

- формирует ключевые дистрибутивы для Абонентских пунктов вместе с паролем доступа к ним;
- по завершению обозначенных работ уведомляет об этом Претендента посредством электронной почты.

Претендент, для получения ключевых дистрибутивов и пароля доступа к ним, должен:

- Предоставить в адрес Оператора копию приказа о назначении Локального Администратора (Приложение №2);
- Направить к Оператору Локального Администратора защищенной сети с доверенностью на получение ключевого дистрибутива (Приложение № 3).

После получения ключевых дистрибутивов Претендент считается Участником.

Факт выдачи ключевого дистрибутива заносится в Журнал учета выдачи ключевых дистрибутивов (Приложение № 4).

4. Порядок изменения направлений связи и/или предоставления доступа к информационным системам

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

- заявительная стадия;
- стадия рассмотрения заявления;
- формирование и передача ключевой информации;
- формирование и передача учётных записей для доступа к информационным системам.

Заявительная стадия.

Участник желающий изменить направление связей и/или получить доступ к информационным системам Защищённой сети направляет в адрес Оператора заявление за подписью руководителя (Приложение №5) и копию документа подтверждающего согласие Владельца информационной системы на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является Оператор - не требуется).

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

Рассмотрение заявки.

Оператор в течение 3-х рабочих дней со дня получения рассматривает заявку, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным системам Защищённой сети.

Решение об изменении направлений связи и/или организации доступа к информационным системам Защищённой сети, направляется в письменной форме в адрес Участника в течение 3-х рабочих дней со дня принятия указанного решения.

Оператор имеет право отказать Участнику в изменении направлений связи и/или организации доступа к информационным системам Защищённой сети, объяснив причину отказа. Решение об отказе в изменении направлений связи и/или организации доступа к информационным системам Защищённой сети направляется в письменной форме в адрес Участника в течение 3-х рабочих дней со дня принятия указанного решения.

Формирование и передача ключевой информации

В течение 5 рабочих дней со дня уведомления Участника о принятии решения об изменении направлений связи и/или организации доступа к информационным системам Защищённой сети Оператора:

- вносит изменения в направления связей между Абонентскими пунктами, в соответствии с заявлением;
- формирует необходимую справочную и ключевую информацию;
- через Центр управления сетью направляет справочную и ключевую информацию на соответствующие Абонентские пункты Участника;
- по завершению обозначенных работ уведомляет об этом Участника.

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

Формирование и передача учётных записей для доступа к информационным системам. Локальный администратор Владельца информационной системы формирует учётные записи для доступа к информационным системам и передаёт их Локальному администратору Участника в сроки и на согласованных ранее условиях.

5. Организация межсетевого взаимодействия с другими сетями ViPNet

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

- заявительная стадия;
- рассмотрение заявления;
- формирование и передача ключевой информации;

Заявительная стадия.

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

Рассмотрение заявления.

Оператор в течение 3-х рабочих дней со дня получения информационного письма проводит оценку оснований и технической возможности для организации межсетевого взаимодействия.

Оператор имеет право отказать в организации межсетевого взаимодействия, объяснив причину отказа.

В случае принятия решения об организации межсетевого взаимодействия Оператор в течение 5-ти рабочих дней в письменной форме уведомляет о принятии такого решения организацию, инициирующую данное взаимодействие.

Формирование и передача ключевой информации.

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

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

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

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

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

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

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

6. Порядок организации межсетевого взаимодействия в случае плановой смены межсетевого мастер-ключа.

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

Предварительные организационные мероприятия.

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

- выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;
- в случае использования симметричного мастер-ключа выбирается сеть, в которой будет создан новый межсетевой мастер-ключ;
- выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для Абонентских пунктов сетей.

Формирование нового межсетевого мастер-ключа.

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

Процедура создания экспорта и приёма импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных и приём импортированных данных в соответствии с «Руководством администратора. ViPNet Administrator [Центр управления сетью]» и «Руководством администратора. ViPNet Administrator [Удостоверяющий и ключевой центр]».

Межсетевое взаимодействие после смены межсетевого мастер-ключа.

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

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

7. Компрометация ключей

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

- посторонним лицам мог стать доступен (стал доступен) файл ключевого дистрибутива Абонента;
- посторонним лицам мог стать доступен (стал доступен) съёмный носитель ключевой информации Абонента;

- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте;
- на Абонентском пункте отсутствовал (был отключен) модуль ViPNet Client Monitor, или он устанавливался в 4-й или 5-й режим, и в локальной сети считается возможным присутствие посторонних лиц;
- прекращение полномочий Абонента или Локального администратора, согласно соответствующего приказа, имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора (договора возмездного оказания услуг).

При возникновении сомнений в неизвестности посторонним лицам пароля доступа Абонента при старте модуля ViPNet Client Monitor, при условии, что доступ к Абонентскому пункту посторонних лиц был невозможен, Локальному Администратору следует сменить пароль и разрешить Абонентам продолжить работу.

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

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

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

В случае прекращения полномочий Администратора, ключевая информация всех Абонентов Участника считается скомпрометированной.

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

Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Координатора защищенной сети.

Координатор защищенной сети при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

- в программном обеспечении ViPNet [Администратор] объявить ключи Абонентского пункта скомпрометированными и создать средствами программного обеспечения справочники связей при компрометации с необходимой информацией;
- оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом, ключевая информация которого была скомпрометирована;
- сформировать средствами программного обеспечения ViPNet [Администратор] новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;

- произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищенной сети.

8. Порядок организации межсетевого взаимодействия в случае компрометации ключей

Компрометация ключей Абонента.

При наступлении любого из перечисленных в п. 7 настоящего Регламента событий Абонент, должен немедленно прекратить работу на своём Абонентском пункте и сообщить о факте компрометации администратору своей сети ViPNet.

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

- в программном обеспечении ViPNet [Администратор] объявить ключи Абонентского пункта скомпрометированными и создать средствами программного обеспечения справочники связей при компрометации с необходимой информацией;
- оповестить о факте компрометации ключей всех Абонентов, связанных с Абонентом, ключевая информация которого была скомпрометирована;
- сформировать средствами программного обеспечения ViPNet [Администратор] новую ключевую информацию. Все файлы с новой ключевой информацией зашифрованы на не скомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;
- произвести рассылку сформированных обновлений ключей на Абонентские пункты Защищенной сети.
- сформировать и отправить импорт для сети ViPNet, с Абонентскими пунктами которой, взаимодействовал скомпрометированный Абонентский пункт;

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

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

Внеплановая смена межсетевого мастер-ключа.

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

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

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

9. Порядок разрешения конфликтных ситуаций

Возникновение конфликтных ситуаций может быть связано с формированием, доставкой, получением, подтверждением получения Участниками электронных документов и/или получение доступа к информационным системам других Участников.

Разрешение конфликтных ситуаций осуществляется путём взаимодействия Локальных администраторов Участников, у которых возникли претензии.

Приложение №1
к Регламенту

Директору КУ НАО «НИАЦ»
Е.А. Ружникову

Заявление на подключение к Защищенной виртуальной сети ViPNet
казенного учреждения Ненецкого автономного округа
«Ненецкий информационно-аналитический центр»

Прошу подключить _____
(название организации)
к защищенной виртуальной сети ViPNet казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр» для обмена информацией с _____.

1. Полное наименование организации
2.Сокращенное наименование организации
3. Юридический адрес организации
4. Количество необходимых для регистрации Абонентских пунктов
5. Перечень информационных систем к которым необходим доступ
6. ФИО Локального администратора
7. Контактные телефоны, e-mail Локального администратора

Дата заполнения Подпись руководителя М.П.

Приложение №2
к Регламенту

ПРИКАЗ

«___» _____ 20___ г.

О назначении Администратора защищенной сети.

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и Абонентских пунктов, принадлежащих _____ и относящихся к защищенной виртуальной сети ViPNet казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр»

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором защищенной сети:

- ФИО – должность.

2. В своей работе по выполнению функций Локального администратора защищенной сети руководствоваться:

- Регламентом взаимодействия участников защищенной сети ViPNet казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр»;
- Регламентом работы Удостоверяющего центра казенного учреждения Ненецкого автономного округа «Ненецкий информационно-аналитический центр».

3. Контроль за исполнением приказа _____.

_____	_____	_____
(должность руководителя)	(подпись)	(ФИО)
	М.П.	

Приложение № 3

к Регламенту

Доверенность на получение ключевого дистрибутива

(наименование населенного пункта) «__»_____20__ г.

(Наименование организации) в лице (должность) (фамилия, имя, отчество) уполномочивает:

(фамилия, имя, отчество), (серия и номер паспорта, кем и когда выдан) получить в казенном учреждении Ненецкого автономного округа «Ненецкий информационно-аналитический центр» ключевой дистрибутив для первичного запуска прикладной программного обеспечения ViPNet [Клиент].

Настоящая доверенность действительна по «____» _____ 20___г.

Подпись лица, получившего доверенность _____

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

М.П.

Приложение № 4

к Регламенту

Журнал учета выдачи ключевых дистрибутивов

№ п/п	Дата выдачи	Организация	Идентификатор дистрибутива	Тип носителя	Способ передачи (лично, по доверенности, по защищенным каналам связи…)	Подпись получившего

Приложение №5

к Регламенту

Директору КУ НАО «НИАЦ»

Е.А. Ружникову

ЗАЯВЛЕНИЕ

на изменение направлений связи Защищенной виртуальной сети ViPNet

казенного учреждения Ненецкого автономного округа

«Ненецкий информационно-аналитический центр»

1. Полное наименование организации
2. Наименование Абонентских пунктов (идентификаторы узлов)
1 – Наименование АП №1 (0x000000) 2 – Наименование АП №2 (0x000000) …
3. Направления связи
Участник Защищенной сети 1 Участник Защищенной сети 2 …
4. Операция (добавить, удалить)
5. Контактный телефон, e-mail Локального администратора

_____	_____	_____
(должность руководителя)	(подпись)	(ФИО)
	М.П.	

Приложение №6

к Регламенту

ПРОТОКОЛ

установления межсетевого взаимодействия

«____» _____ 20__г.

1. Межсетевое взаимодействие устанавливается между сетями:

Номер сети	Наименование организации
№ 2440	*казенное учреждение Ненецкого автономного округа «Ненецкий информационно-аналитический центр»*
№_____	*Полное наименование организации*

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

3. Процедуру установления межсетевого взаимодействия осуществляли:

Номер сети	Должность	ФИО
№ 2440		
№_____		

4. Передача начального и ответного экспорта между сетями №2440 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 №2440 - «_____»

в сети №____ - «_____»

7. При установлении межсетевого взаимодействия в части создания связей между сетевыми узлами были произведены импорты справочников из сети №2440 и №___.

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

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

Администратор сети ViPNet №2440	Администратор сети ViPNet №_____
_____ (ФИО)	_____ (ФИО)
_____ (Подпись)	_____ (Подпись)
«_____»_____20__г.	«_____»_____20__г.