УТВЕРЖДАЮ

Директор
ГБУЗ «Республиканский медицинский информационно-аналитический центр» Министерства здравоохранения Республики Бурятия

_____ Э.Д. Батуев

«____» _____ 2018г.

РЕГЛАМЕНТ

ЗАЩИЩЕННОЙ ВИРТУАЛЬНОЙ СЕТИ VIPNET

ГБУЗ «РМИАЦ» МЗ РБ

г. Улан-Удэ
2018

Содержание

1. Термины и определения

Сетевой узел ViPNet — узел, на котором установлено программное обеспечение ViPNet, зарегистрированный в программе ViPNet Центр управления сетью.

Администратор сети ViPNet — организация, осуществляющая общую политику администрирования всей Защищенной сети передачи данных, и определяющая стратегию развития Защищенной сети передачи данных;

Пользователь сети ViPNet — организация, которая используют программное обеспечение ViPNet и имеет ключи для работы с ним.

Файл лицензии — специальный файл *.itcslic или infotecs.reg, в котором зафиксированы ограничения для вашей сети ViPNet.

Дистрибутив ключей — файл с расширением .dst, создаваемый в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сетевого узла ViPNet. Содержит справочники, ключи и файл лицензии, необходимые для обеспечения первичного запуска и последующей работы программы ViPNet на сетевом узле. Для обеспечения работы программы ViPNet дистрибутив ключей необходимо установить на сетевой узел.

Межсетевое взаимодействие — информационное взаимодействие, организованное между сетями ViPNet. Позволяет сетевым узлам различных сетей ViPNet обмениваться информацией по защищенным каналам.

Направления связи — связи между узлами ViPNet, определяющие возможность защищенного обмена данными.

Защищенная сеть передачи данных — ведомственная защищенная сеть Министерства здравоохранения Республики Бурятия, функционирующая на базе сети ViPNet № 2150 и представляющая собой совокупность сетевых узлов - абонентских пунктов, программных и программно-аппаратных серверов-маршрутизаторов (координаторов), а также средств централизованного мониторинга и управления.

Информационная система — совокупность содержащихся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств;

Ключевой носитель — носитель, содержащий один или несколько дистрибутивов ключей;

Конфиденциальная информация — сведения, независимо от формы их представления, которые не могут быть переданы лицом, получившим доступ к данным сведениям, третьим лицам без согласия их владельца, а также информация, доступ к которой ограничен в соответствии с действующим законодательством РФ;

Компрометация ключей — утрата доверия к тому, что используемые ключи обеспечивают безопасность информации (целостность, конфиденциальность, подтверждение авторства, невозможность отказа от авторства).

Несанкционированный доступ — доступ к информации, хранящейся на различных типах носителей, в базах данных, файловых хранилищах путем изменения (повышения, фальсификации) своих прав доступа;

Сервер-маршрутизатор (Координатор) — программный или программно-аппаратный комплекс, выполняющий функции межсетевого экрана и криптографического шлюза в Защищенной сети передачи данных, а также абонентский пункт без почтовой функции;

Мастер-ключ — ключ, который администратор сети ViPNet использует для формирования симметричных ключей пользователей и узлов. Мастер-ключ формируется с помощью датчика случайных чисел. Он хранится в программе ViPNet Удостоверяющий и ключевой центр в полной секретности, поскольку компрометация мастер-ключа приводит к компрометации всех ключей, сформированных на его основе.

Ответственный пользователь СКЗИ — сотрудник Пользователя сети ViPNet, контролирующее эксплуатацию средства криптографической защиты информации, входящих в состав ЗСПД и находящихся в сегменте Участника.

Пользователь СКЗИ — сотрудник организации Пользователя сети ViPNet эксплуатирующий средства криптографической защиты информации.

2. Сокращения

АРМ – Автоматизированное рабочее место

ЗСДП – Защищенная сеть передачи данных

СКЗИ – Средство криптографической защиты информации

IP – Internet Protocol

MPLS – Multiprotocol label switching

NAT – Network Address Translation

3. Общие положения

3.1 Настоящий Регламент определяет порядок использования Защищенной сети передачи данных ViPNet №2150 и обязателен для исполнения всеми участниками процесса.

3.2 Настоящий Регламент разработан в соответствии с Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных», от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. N 152.

3.3 Администрирование ЗСПД осуществляется специалистами Государственного бюджетного учреждения здравоохранения «Республиканский медицинский информационно-аналитический центр» Министерства здравоохранения Республики Бурятия.

3.4 Прием заявок, предусмотренных п.8-10 данного регламента осуществляется в форме электронной сканированной копии документов по электронной почте на адрес vipnet@burmiac.ru.

3.5 Действующий текст регламента размещен (опубликован) в сети Интернет на портале по адресу: www.burmiac.ru.

3.6 Регламент начинает действовать с момента получения Заявки на подключение.

3.7 Администратор ЗСДП имеет право в одностороннем порядке вносить изменения (дополнения) в настоящий Регламент.

3.8 При возникновении вопросов, не урегулированных положениями настоящего Регламента, следует руководствоваться действующим законодательством РФ.

3.9 Регламент определяет и устанавливает:

- порядок подключения к ЗСПД;
- порядок изменения доступа к информационным системам (направлений связи);
- порядок изменения имени сетевого узла;
- порядок повторного выпуска дистрибутива ключей;
- порядок перевода лицензий в другую сеть;
- порядок смены мастер-ключей;
- порядок отключения сетевых узлов;
- порядок компрометации ключей.

4. Структура и состав Защищенной сети передачи данных

4.1 Защищенная сеть передачи данных представляет собой территориально распределенную информационно-телекоммуникационную сеть, объединяющую сетевые узлы Пользователей сети по технологии ViPNet.

4.2 Связь сетевых узлов Пользователей сети ViPNet осуществляется по имеющимся каналам связи.

4.3 Программное обеспечение, обеспечивающее функционирование ЗСПД:

- ViPNet [Администратор];
- ViPNet [Координатор];
- ViPNet [Клиент];

4.4 В зависимости от количества используемых в подключаемой организации сетевых узлов (АРМ, серверов, терминалов) обрабатывающих подлежащую защите информацию, рекомендуется использовать типы оборудования:

Тип	Количество АРМ, серверов, терминалов в защищаемом сегмента	Рекомендуемое оборудование ViPNet
1	более 500	HW2000
2	от 10 до 500	HW1000
3	от 6 до 10	HW100
4	до 6	ViPNet Client

4.5 Максимальное допустимое количество ViPNet Client у Пользователя сети ViPNet, напрямую подключенных к координатору Администратора сети ViPNet должно быть не больше 10. При превышение данного количества, Пользователь сети ViPNet, должен приобрести координатор.

5. Функции и полномочия Администратора сети ViPNet

5.1 Обязанности Администратора сети ViPNet:

- разработка единых правил формирования, развития и функционирования ЗСПД;
- разработка регламентирующих документов использования информационных систем, доступ к которым предоставляется с использованием ЗСПД;
- проведение мероприятий по модернизации и развитию ЗСПД;
- своевременное реагирование на поступившие заявки о неисправностях в работе компонентов ЗСПД и принятие необходимых мер по их устранению;
- периодические проверки состояния ЗСПД и своевременное реагирование на попытки несанкционированного доступа;
- информирование Пользователей сети ViPNet о порядке работы и ответственности за нарушение настоящего Регламента;
- информирование Пользователей сети ViPNet о проводимых работах по обслуживанию и возможных перебоях в работе Защищенной сети;

5.2 Права Администратора сети ViPNet:

- информировать руководителей Пользователей сети ViPNet при невыполнении их работниками требований безопасности и несоблюдения других требований по обеспечению бесперебойного функционирования ЗСПД;
- принимать решение об отключении или ограничении доступа к информационным системам ЗСПД в случаях нарушения Пользователями сети ViPNet требований настоящего Регламента Защищенной сети ViPNet.

5.3 Ответственность Администратора сети ViPNet:

- невыполнение требований настоящего Регламента, а также других актов, регулирующих работу ЗСПД;
- несвоевременное выявление попыток несанкционированного доступа, приведших к нарушению требований по безопасности и сбою её функционирования;
- несвоевременное устранение неисправностей в работе компонентов ЗСПД;
- неправомерное использование информации, циркулирующей в ЗСПД, к которой Администратор получает доступ в связи с выполнением своих функций.

6. Функции и полномочия Пользователя сети ViPNet

6.1 Обязанности Пользователя сети ViPNet:

- подключение сетевых узлов ViPNet и информационных систем к ЗСПД;
- вести учет имеющихся у него лицензий и предоставлять их копии по требованию Администратора сети ViPNet;
- оплачивать за свой счет сети передачи данных, необходимые для работы Защищенной сети передачи данных;
- обеспечивать работоспособность программного обеспечения, СКЗИ, необходимых для информационного обмена;
- использовать сертифицированные средства защиты информации;
- выполнять требований формуляров на СКЗИ и иных нормативных документов, регламентирующих эксплуатацию средств криптографической защиты информации;
- назначить ответственного пользователя СКЗИ;
- информировать работников Пользователя сети ViPNet о порядке работы в ЗСПД и ответственности за нарушение данного Регламента;
- принимать меры по пресечению несанкционированного доступа к компонентам ЗСПД Пользователя сети ViPNet;
- уведомлять Администратора сети ViPNet о случаях нарушений и принятых мерах;
- приобретать техническую поддержку для сетевых узлов ViPNet, принадлежащих Пользователю сети ViPNet.

6.2 Права Пользователя сети ViPNet:

- сообщать Администратору сети ViPNet о действиях, связанных с несанкционированным доступом к ресурсам ЗСПД или о нарушениях других требований по обеспечению безопасности информации и бесперебойной работы ЗСПД;

- предоставлять Администратору сети ViPNet предложения, касающиеся разработки единых правил формирования, развития и работы ЗСПД.

6.3 Ответственность Пользователя сети ViPNet:

- невыполнение требований настоящего Регламента, а также других актов, регулирующих работу ЗСПД;
- несвоевременное выявление попыток несанкционированного доступа, приведших к нарушению требований по безопасности ЗСПД и сбою её функционирования;
- несвоевременное устранение неисправностей в работе компонентов ЗСПД.

7. Технические мероприятия

7.1 Для подключения ViPNet [Координатор] на территории Пользователя сети ViPNet должны быть обеспечены:

7.1.1 подключение к одному из каналов передачи данных:

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

7.1.2 подключение к сетевому оборудованию Пользователя сети ViPNet интерфейсов координатора с использованием интерфейсов Ethernet Base T 100/1000;

7.1.3 доступность внешнего интерфейса координатора из сети Интернет одним из следующих способов:

- обеспечить NAT-трансляцию приватного IP-адреса в публичный IP-адрес (трафик по протоколу UDP, порт 55777);
- выделить для интерфейса публичный IP-адрес.

7.1.4 маршрутизация в локальной сети Пользователя сети ViPNet должна осуществляться таким образом, чтобы трафик, отправляемый на серверы Администратора сети ViPNet, направлялся на внутренний интерфейс координатора;

7.1.5 отсутствие логических препятствий для прохождения трафика по порту UDP 55777 между внешним интерфейсом координатора и адресом координатора Администратора сети ViPNet.

7.2 Для подключения ViPNet [Клиент] на территории Пользователя сети ViPNet должны быть обеспечены:

7.2.1 подключение к одному из каналов передачи данных:

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

7.2.2 отсутствие логических препятствий для прохождения трафика по порту UDP 55777 между внешним интерфейсом координатора и адресом координатора Администратора сети ViPNet.

7.3 При возникновении технической неисправности оборудования ЗСПД у Пользователя сети ViPNet, Пользователь сети ViPNet отправляет заявку в техническую поддержку продуктов ViPNet (компания «ИнфоТеКС» или аффилированные лица).

7.4 В случае возникновения производственной необходимости проведения аварийных и планово-профилактических работ, ЗСПД может быть закрыта для доступа.

7.5 О проведение работ Администратор сети ViPNet уведомляет Пользователей сети ViPNet не менее чем за 24 часа, до намеченного срока начала работ.

8. Порядок организации подключения пользователей к ЗСПД

8.1 Организация подключения к ЗСПД включает в себя следующие стадии:

- подача заявки;
- стадия рассмотрения заявки;
- приобретение программного обеспечения;
- формирование и передача ключевой информации.

8.2 Участник, желающий подключиться к ЗСПД (далее - Претендент) направляет в соответствии с п. 3.4 в адрес Администратора сети ViPNet заявку о намерении подключиться к ЗСПД (Приложение 1).

8.3 Стадия рассмотрения заявки

8.3.1 Администратор сети ViPNet в течении 5-ти рабочих дней со дня получения заявления о намерении подключиться к ЗСПД, проводить оценку оснований для подключения Претендента к ЗСПД, технической возможности организации направлений связи и доступа к информационным системам.

8.3.2 Приобретение программного обеспечения ViPNet, до рассмотрения заявления не является основанием и гарантией подключения Претендента к ЗСПД.

8.3.3 Администратор сети ViPNet уведомляет Претендента по электронной почте, указанной в заявлении о принятии решения о подключении (отказе в подключении) к Защищенной сети, в течение 3-х рабочих дней со дня принятия указанного решения.

8.4 Приобретение программного обеспечения

8.4.1 В случае принятия положительного решения о подключении к ЗСПД, Претендент самостоятельно приобретает лицензии для программного обеспечения ViPNet и дистрибутив.

8.4.2 При оформлении договорных отношений по приобретению программного обеспечения ViPNet Претендент указывает номер сети для подключения – 2150.

8.4.3 Подключение Претендента к ЗСПД осуществляется Администратором сети ViPNet, только после получения файла лицензии от производителя программного обеспечения или представителя производителя программного обеспечения.

8.4.4 Администратор сети ViPNet уведомляет Претендента о получении файла лицензии, по электронной почте, указанной в заявлении о намерении подключиться к ЗСПД.

8.5 Формирование ключевой информации

8.5.1 Претендент после получения информации о поступлении файла лицензии, формирует и направляет в Администратору сети ViPNet заявку на изготовление дистрибутива ключей (Приложение 2).

8.5.2 В течении 3 рабочих дней со дня получения от Претендента заявки на подключение Администратор сети ViPNet:

- Производит регистрацию сетевых узлов в Центре управления сетью;
- Организовывает направления связи между сетевыми узлов, в соответствии с заявкой на подключении;
- Формирует дистрибутивы ключей для сетевых узлов вместе с паролем доступа к нему;
- По завершению обозначенных работ уведомляет об этом Претендента.

8.6 Передача дистрибутива

8.6.1 Дистрибутив ключей передается ответственному лицу организации Претендента при предъявлении доверенности на получение ключевой информации с указанием количества получаемых дистрибутивов ключей и удостоверения личности.

8.6.2 Ключевая информация записывается на флеш-накопитель ответственного лица и передается наручно или иным доверенным способом.

8.6.3 Факт выдачи дистрибутива ключей, заносится в Журнал учёта выдачи ключевых документов.

9. Порядок изменения имени сетевого узла ViPNet или доступа к информационным системам (направлений связи)

9.1 Для проведения модификации доступа к информационным системам (направлений связи) или изменения имени сетевого узла необходимо выполнение следующих технологических и организационных мероприятий:

9.1.1 Пользователь сети ViPNet формирует универсальную заявку на изменение доступа (Приложение 3) или заявку на изменение имени сетевого узла (Приложение 4) и направляет её в соответствии с п. 3.4 в адрес Администратор сети ViPNet;

9.1.2 Администратор сети ViPNet в течение 2-х рабочих дней со дня получения рассматривает заявку, проводит оценку технической возможности для изменения доступа к информационным системам (направлений связи) или изменение имени сетевого узла ViPNet.

9.1.3 В течение 2 рабочих дней со дня принятии решения об изменении направлений связи ЗСПД Администратор сети ViPNet вносит изменения в направления связей между сетевыми узлами, в соответствии с заявлением (в случае изменения направления связи);

9.1.4 Администратор сети ViPNet уведомляет Пользователя сети ViPNet по электронной почте, указанной в заявлении об изменении доступа или имени сетевого узла.

9.2 Администратор сети ViPNet имеет право отказать Пользователю сети ViPNet в изменении направлений связи сетевого узла ЗСПД, объяснив причину отказа. Решение об отказе в изменении направлений связи или изменение имени направляется в письменной форме в адрес Пользователя сети ViPNet в течение 3-х рабочих дней со дня принятия указанного решения.

9.3 Положения данного раздела не распространяются на порядок предоставления доступа к информационным системам или изменения направлений связи при осуществлении межсетевого взаимодействия.

10. Порядок повторного выпуска дистрибутива ключей

10.1 Пользователь сети ViPNet для повторного получения дистрибутива ключей направляет в соответствии с п. 3.4 в адрес Администратора сети ViPNet заявку на повторный выпуск дистрибутива ключей (Приложение 5).

10.2 Администратор сети ViPNet в течение 2-х рабочих дней со дня получения рассматривает заявку.

10.3 В случае если повторный выпуск дистрибутива ключей необходим в связи с компрометацией ключевой информации, перед выпуском дистрибутива ключей проводятся мероприятия в соответствии с п. 14.

10.4 В течение 2 рабочих дней со дня принятии решения о повторном выпуске дистрибутивов ключей Администратор сети ViPNet осуществляет выпуск дистрибутивов ключей и уведомляет об этом Пользователя сети ViPNet, по электронной почте.

10.5 Порядок получения дистрибутивов ключей указан в п 8.6.

11. Перенос сетевого узла ViPNet в другую сеть

11.1 Пользователь сети ViPNet, по согласованию с Администратором сети ViPNet, может перенести принадлежащие им лицензии на сетевые узлы ViPNet в другую сеть.

11.2 Пользователь сети ViPNet для отключения от ЗСПД направляет в соответствии с п. 3.4 в адрес Администратора сети ViPNet заявление о прекращении использования подключения к защищенной сети передачи данных (Приложение 6).

11.3 По результатам проведения проверки достоверности сведений, указанных в предоставленных документах для идентификации и отключения от ЗСПД, Администратором сети ViPNet выносится решение об отключении пользователя СКЗИ от защищенной сети передачи данных или об отказе в таком отключении.

11.4 В случае принятия решения об отключении от ЗСПД, Администратор сети ViPNet в течении двух рабочих дней уведомляет Пользователя сети ViPNet.

11.5 В случае принятия решения об отказе в отключении от ЗСПД, Администратор сети ViPNet в течение трех рабочих дней направляет Пользователю сети ViPNet мотивированный отказ.

12. Порядок смены мастер-ключей

12.1 Смена мастер-ключей влечет за собой смену всех ключей в сети ViPNet. Она может быть, как плановой, так и внеплановой. Плановая смена мастер-ключей проводится с определенной периодичностью один раз в год. Внеплановая смена мастер-ключей производится при компрометации ключей.

12.2 Перед проведением смены мастер-ключей Администратор сети ViPNet уведомляет за 2 недели Пользователей сети ViPNet.

12.3 Пользователь сети ViPNet в период смены мастер ключей обязан обеспечить работоспособность сетевых узлов ViPNet и проследить за принятием этими сетемыми узлами ключевой и справочной информацией.
12.4 После смены мастер-ключей первичная инициализация с использованием выданных до даты смены мастер-ключей дистрибутивов ключей будет невозможна.

13. Компрометация ключей

13.1 К событиям компрометации, когда ключи Пользователя сети ViPNet считаются скомпрометированными, относятся следующие случаи:

- посторонним лицам мог стать доступен (стал доступен) файл ключевого дистрибутива;
- посторонним лицам мог стать доступен (стал доступен) съёмный носитель ключевой информации;
- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на сетевом узле;
- на сетевом узле 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 ответственного пользователя СКЗИ, согласно соответствующему приказу, имевшего доступ к паролям и ключам, в том числе в связи с расторжением трудового договора (договора возмездного оказания услуг).

13.2 При возникновении любого из перечисленных событий Пользователь сети ViPNet должен немедленно прекратить работу на скомпрометированном сетевом узле и сообщить о факте компрометации или предполагаемом факте компрометации Администратору сети ViPNet.

13.3 По факту компрометации ключей должно быть проведено служебное расследование.

13.4 Администратор сети ViPNet в случае компрометации ключей пользователя СКЗИ проводит процедуру внеплановой смены ключей данного пользователя, для которой необходимо выполнение следующих технологических и организационных мероприятий:

- Администратор сети ViPNet объявляет ключи данного пользователя скомпрометированными;
- Администратор сети ViPNet формирует новую ключевую информацию, как для скомпрометированного пользователя СКЗИ, так и для всех пользователей СКЗИ, с которыми он был связан;
- Администратор сети ViPNet отправляет новую ключевую информацию пользователям СКЗИ, с которыми он был связан;
- Администратор сети ViPNet передает Пользователю сети ViPNet дистрибутив ключей в соответствии с п. 8.6;
- После обновления ключевой информации на всех взаимодействующих сетевых узлах, пользователи СКЗИ данных сетевых узлов могут продолжать свою работу.

14. Ответственность за нарушения данного регламента

В случае нарушения требований данного Положения, послуживших причиной сбоя функционирования ЗСПД или несанкционированного доступа к информации, циркулирующей в ЗСПД, все категории пользователей несут ответственность в соответствии с действующим законодательством.

Приложение 1

Оформляется на официальном бланке организации!

О подключении
к защищённой виртуальной сети ViPNet

Прошу рассмотреть возможность подключить:

_____
_____
название организации

к защищённой виртуальной сети ViPNet 2150 МИАЦ Республики Бурятия для:

_____
_____
_____
обоснование необходимости подключения

Предполагаемое число подключаемых сетевых узлов – _____.

Перечень информационных систем, к которым необходим доступ:

_____
_____

Лицо, ответственное за подключение, и контактный телефон:

_____
_____

_____	_____	_____
[Должность руководителя]	[подпись]	Ф.И.О.

«____» _____201_ г.

М.П.

Отметка об
Исполнителе

Приложение 2

Оформляется на официальном бланке организации!

ЗАЯВКА
на изготовление ключевой информации для подключения к Защищённой сети ViPNet №2150

Полное наименование организации	
Сокращённое название организации	
Количество и адреса установки абонентских пунктов	
Номер заявки	
ФИО ответственного пользователя СКЗИ	
Контактные телефоны ответственного пользователя СКЗИ	
Контактный E-mail ответственного пользователя СКЗИ	

[Должность руководителя]	[подпись]	Ф.И.О.

«____» _____201_ г.

М.П.

Отметка об
Исполнителе

Приложение 3

Оформляется на официальном бланке организации!

ЗАЯВКА
Защищённая сеть передачи данных ViPNet №2150

☐	На изменение доступа к информационным системам	☐	На изменение направления связи (Деловая почта)

Нужное отметить

☐	Предоставление доступа/добавление связей	☐	Прекращение доступа/удаление связей

Нужное отметить

Полное наименование организации без сокращений (на основании учредительных документов)
Имя сетевого узла ViPNet, которому изменяется доступ/направления связи:
Перечень информационных ресурсов, к которым необходим доступ/направление связи:
Обоснование изменения связи для защищенного обмена информацией/ предоставления доступа к защищенным ресурсам
Контактный телефон/e-mail

[Должность руководителя]	[подпись]	Ф.И.О.

«____» _____201_ г.

М.П.

Отметка об
Исполнителе

Приложение 4

Оформляется на официальном бланке организации!

Прошу рассмотреть возможность изменить имя сетевого узла:

Текущее название сетевого узла
Новое название сетевого узла
Обоснование для изменения имени сетевого узла
Контактный телефон/e-mail

[Должность руководителя]	[подпись]	Ф.И.О.

«____» _____201_ г.

Отметка об
Исполнителе

Приложение 5

Оформляется на официальном бланке организации!

Прошу осуществить повторное создание дистрибутива ключей для первичной инициализации сетевого узла сети ViPNet:

Название сетевого узла
Обоснование для перевыпуска дистрибутива ключей
☐ Компрометация ☐ Потеря работоспособности ☐ Другое (указать ниже): _____
Контактный телефон/e-mail

_____ _____ _____

[Должность руководителя] [подпись] Ф.И.О.

«____» _____201_ г.

Отметка об
Исполнителе

Приложение 6

Оформляется на официальном бланке организации!

Прошу согласовать перенос сетевого узла ViPNet сети 2150 в связи с:

Название переносимого сетевого узла
Обоснование для переноса сетевого узла
Контактный телефон/e-mail

[Должность руководителя]	[подпись]	Ф.И.О.

«____» _____201_ г.

Отметка об
Исполнителе