**УПРАВЛЕНИЕ ДЕЛАМИ ГЛАВЫ И ПРАВИТЕЛЬСТВА КАБАРДИНО-БАЛКАРСКОЙ РЕСПУБЛИКИ**

**КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ И ГЭТАЩХЬЭМРЭ ПРАВИТЕЛЬСТВЭМРЭ Я ГУЭХУХЭМКІЭ УПРАВЛЕНЭ**
**КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ БЫШЧЫСЫНЫ БЛА ПРАВИТЕЛЬСТВОСУНУ ИШЛЕРИНИ УПРАВЛЕНИЯСЫ**

# ПРИКАЗ

9 мая 2017 г. 6

## О Регламенте функционирования единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления

В соответствии с постановлением Правительства Кабардино-Балкарской Республики от 8 июля 2016 г. № 126-ПП «О единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления» **п р и к а з ы в а ю:**

1. Утвердить прилагаемый Регламент функционирования единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления.

2. Отделу технической защиты информации департамента информационных технологий Управления делами Главы и Правительства Кабардино-Балкарской Республики обеспечить функционирование единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления в режиме промышленной эксплуатации.

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

4. Контроль за исполнением настоящего приказа оставляю за собой.

Управляющий делами
Главы и Правительства
Кабардино-Балкарской Республики З.Калов

Управление делами Главы и Правительства КБР
СЕКРЕТАРИАТ

УТВЕРЖДЕН
приказом Управления
делами Главы и Правительства
Кабардино-Балкарской Республики
от 2 мая 2017г. № 6

# РЕГЛАМЕНТ
## функционирования единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления

### 1. Общие положения

1.1. Настоящий Регламент определяет порядок функционирования единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления (далее – ЕЗСПД). ЕЗСПД является единой информационной коммуникационной средой органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления, созданной в целях обеспечения функционирования региональной системы электронного межведомственного взаимодействия, перехода исполнительных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления к предоставлению услуг в электронной форме на основе межведомственного взаимодействия, перехода на систему юридически значимого электронного документооборота, обеспечения государственных и муниципальных служащих Кабардино-Балкарской Республики, участвующих в предоставлении государственных и муниципальных услуг и осуществляющих юридически значимые действия, средствами электронной подписи.

1.2. Регламент функционирования ЕЗСПД (далее – Регламент) разработан в соответствии с:

Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;

постановлением Правительства Кабардино-Балкарской Республики от 8 июля 2016 г. № 126-ПП «О единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления».

1.3. Регламент определяет и устанавливает:

порядок организации и подключения органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления и иных организаций к ЕЗСПД;

порядок предоставления доступа к информационным системам ЕЗСПД;

права и обязанности администраторов и пользователей ЕЗСПД;

порядок функционирования и технического обслуживания компонентов ЕЗСПД;

порядок организации защищённого межсетевого взаимодействия;

порядок разрешения конфликтных ситуаций.

1.4. Для целей настоящего Регламента используются следующие основные понятия:

ViPNet-Администратор – программное обеспечение, предназначенное для конфигурирования и управления виртуальной защищённой ViPNet-сетью;

ViPNet-Клиент – программное обеспечение, реализующее на рабочем месте пользователя или сервере функцию VPN-клиента, персонального экрана и клиента защищённой почтовой службы;

ViPNet-Координатор – программно-аппаратный комплекс или программное обеспечение, выполняющее функции универсального сервера виртуальной ViPNet-сети;

ViPNet-сеть – виртуальная защищенная сеть, построенная путём использования системы персональных и межсетевых экранов на защищаемых компонентах распределённой сети и объединения защищаемых элементов через виртуальные соединения (туннели), обеспечивающие шифрование сетевого трафика между этими элементами;

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

Абонент – сотрудник Участника ЕЗСПД, использующий для выполнения своих служебных обязанностей сервисы и информационные системы ЕЗСПД;

Абонентский пункт – персональный компьютер с установленным программным обеспечением ViPNet-Клиент;

Владелец информационных систем – Участник ЕЗСПД, осуществляющий владение и пользование информационными системами и реализующий полномочия распоряжения в пределах, установленных законодательством;

Главный администратор (Уполномоченный сотрудник) – сотрудник Оператора ЕЗСПД, осуществляющий общую политику администрирования всей ЕЗСПД;

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

Ключевой носитель – носитель, содержащий один или несколько ключей;

Компрометация ключа – утрата доверия к тому, что используемые ключи обеспечивают безопасность информации;

Координатор – сотрудник Оператора ЕЗСПД, определяющий общую стратегию развития ЕЗСПД;

Локальный администратор – назначенный приказом сотрудник Участника ЕЗСПД, осуществляющий администрирование информационных систем и абонентских пунктов, принадлежащих данному Участнику ЕЗСПД;

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

Список отозванных сертификатов – документ на бумажном носителе или электронный документ с электронной подписью Уполномоченного лица Удостоверяющего центра, содержащий список сертификатов, действие которых прекращено или приостановлено до истечения срока их действия.

Средство электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи. В ЕЗСПД, данные функции реализованы в модуле «Деловая почта»;

Удостоверяющий ключевой центр (УКЦ) – составная часть программного обеспечения ViPNet-Administrator, которое используется для администрирования ViPNet-сети, а также для выполнения функций удостоверяющего центра: издания и обслуживания сертификатов ключа проверки электронной подписи;

Участник ЕЗСПД – орган государственной власти Кабардино-Балкарской Республики, орган местного самоуправления, подведомственные органы, иные организации, подключаемые к ЕЗСПД.

Центр управления сетью (ЦУС) – аппаратные или программные средства для мониторинга, конфигурирования и управления узлами ViPNet-сети;

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

## 2. Порядок организации подключения Участников к ЕЗСПД

2.1 Организация подключения органа государственной власти Кабардино-Балкарской Республики или органа местного самоуправления, подведомственной или иной организации к ЕЗСПД включает в себя следующие стадии:

стадия заключения соглашения о доступе к ЕЗСПД;

закупка программного обеспечения и/или программно-аппаратного комплекса;

заявительная стадия;

стадия рассмотрения заявления;

формирование и передача ключевой информации;

формирование и передача учётных записей для доступа к информационным системам.

2.2. Стадия заключения соглашения о доступе к ЕЗСПД.

Орган государственной власти Кабардино-Балкарской Республики, орган местного самоуправления или иная организация, желающая подключиться к ЕЗСПД (далее – Претендент), обязана заключить соглашение с Оператором ЕЗСПД.

2.3. Закупка программного обеспечения ViPNet-Клиент и/или ViPNet-Координатор Претендентом.

2.3.1. После заключения соответствующего соглашения Претендент самостоятельно приобретает программное обеспечение ViPNet-Клиент и/или ViPNet-Координатор.

2.3.2. При оформлении договорных отношений по приобретению программного обеспечения ViPNet-Клиент и/или ViPNet-Координатор Претендент указывает номер ViPNet-сети для подключения – 1465.

2.4. Заявительная стадия.

Претендент направляет в адрес Оператора ЕЗСПД заявление о намерении подключиться к ЕЗСПД (приложение №1).

2.4.1. В заявлении должна содержаться следующая информация:

точное количество подключаемых Абонентских пунктов;

подробная схема сети Претендента с указанием всех IP-адресов в том числе запланированных для подключения;

общий перечень Участников ЕЗСПД, с которыми необходима организация защищённого обмена;

полный перечень информационных систем, к которым необходимо организовать доступ;

тип подключения к сети Интернет или иной сети передачи данных с указанием сведений о провайдере и используемом оборудовании;

заверенная Претендентом копия документа, подтверждающего законное приобретение программного обеспечения VipNet (Договор/Контракт);

Ф.И.О., контактный телефон и адрес электронной почты лица, ответственного за подключение Претендента.

2.5. Стадия рассмотрения заявления.

2.5.1. Оператор ЕЗСПД в течение пяти рабочих дней со дня получения заявления о намерении подключиться к ЕЗСПД проводит оценку правильности заполнения всех документов, оснований для подключения Претендента к ЕЗСПД, технической возможности организации направлений связи, доступа к информационным системам.

2.5.2. Решение о подключении Претендента к ЕЗСПД направляется в письменной форме в адрес Претендента в течение трех рабочих дней со дня принятия указанного решения.

2.5.3. Оператор ЕЗСПД имеет право отказать Претенденту в подключении к ЕЗСПД, объяснив причину отказа. Решение об отказе в подключении Претендента к ЕЗСПД направляется в письменной форме в адрес Претендента в течение трех рабочих дней со дня принятия указанного решения.

2.5.4. Оператор ЕЗСПД уведомляет Претендента о принятии решения о подключении (отказе в подключении) к ЕЗСПД посредством электронной почты, указанной в заявление о намерении подключиться к ЕЗСПД, со ссылкой на соответствующее решение.

2.5.5. Подключение Претендента к ЕЗСПД осуществляется Оператором ЕЗСПД, только после получения регистрационных файлов от производителя программного обеспечения или представителя производителя программного обеспечения, о чем лицу, ответственному за подключение сообщается в течение двух рабочих дней с момента получения регистрационных файлов.

2.5.6. Оператор ЕЗСПД вправе отказать в подключении к ЕЗСПД в случае предоставления Претендентом неполных или неточных данных.

2.6. Формирование и передача ключевой информации.

2.6.1. Оператор ЕЗСПД в течение трех рабочих дней со дня получения регистрационных файлов:

производит регистрацию Абонентских пунктов и Абонентов в Центре управления сетью;

организовывает направления связи между Абонентскими пунктами в соответствии с заявкой на подключение;

формирует дистрибутивы ключей для Абонентских пунктов вместе с паролем доступа к нему;

по завершении обозначенных работ уведомляет об этом Претендента.

2.6.2. В случае заявки на изготовление более 5 абонентских пунктов срок выполнения пункта 2.6.1 увеличивается пропорционально количеству абонентских пунктов из расчета каждые 5 абонентских пунктов на 1 день.

2.6.3. Претендент для получения дистрибутива ключей и пароля доступа к нему должен:

а) предоставить Оператору ЕЗСПД:

копии приказов о назначении Локального администратора (приложение № 2) и Абонентов ЕЗСПД (приложение № 3);

копии соглашений с Локальным администратором и Абонентами ЕЗСПД о неразглашении информации, к которой будет получен доступ в связи с выполнением функций (приложение № 4);

б) направить к Оператору ЕЗСПД Локального администратора или ответственного сотрудника с доверенностью на получение дистрибутива ключей (приложение № 5).

2.6.4. Факт выдачи и получения дистрибутива ключей заносится в Журнал учёта ключевых документов.

2.6.5. Претендент для получения доступа к информационным системам Участников ЕЗСПД должен предоставить в адрес Оператора ЕЗСПД копию

документа, подтверждающего согласие Владельца информационной системы (далее – Владельца) на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является Оператор ЕЗСПД, – не требуется).

2.6.6. Оператор ЕЗСПД не несет ответственности за неисполнение требований договорных соглашений и/или сроков исполнения договорных соглашений Претендента в случае соблюдения Оператором ЕЗСПД сроков и процедур, установленных настоящим Регламентом.

## 3. Порядок изменения направлений связи и/или предоставления доступа к информационным системам ЕЗСПД

3.1. 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;

3.2. Заявительная стадия.

3.2.1. Участник ЕЗСПД, желающий изменить направление связи и/или получить доступ к информационным системам ЕЗСПД, направляет в адрес Оператора ЕЗСПД заявку за подписью руководителя (приложение № 6) и копию документа, подтверждающего согласие Владельца на предоставление доступа к информационной системе (в отношении информационных систем, Владельцем которых является Оператор ЕЗСПД,– не требуется).

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

3.3. Рассмотрение заявки.

3.3.1. Оператор ЕЗСПД в течение трех рабочих дней со дня получения рассматривает заявку, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным системам ЕЗСПД.

3.3.2. Решение об изменении направлений связи и/или организации доступа к информационным системам ЕЗСПД направляется в письменной форме в адрес Участника ЕЗСПД в течение трех рабочих дней со дня принятия указанного решения.

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

3.3.4. Оператор ЕЗСПД уведомляет Претендента об изменении направлений связи и/или организации доступа к информационным системам ЕЗСПД, посредством электронной почты, со ссылкой на соответствующее решение.

3.4. Формирование и передача ключевой информации.

3.4.1. В течение пяти рабочих дней со дня уведомления Участника ЕЗСПД о принятии решения об изменении направлений связи и/или организации доступа к информационным системам ЕЗСПД Оператор ЕЗСПД:

вносит изменения в направления связей между Абонентскими пунктами в соответствии с заявлением;

формирует необходимую справочную и ключевую информацию;

через Центр управления сетью, а в случае отсутствия такой возможности иным доверенным способом направляет справочную и ключевую информацию на соответствующие Абонентские пункты Участника ЕЗСПД;

по завершении обозначенных работ уведомляет об этом Участника ЕЗСПД.

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

3.4.3. В случае заявки на изменение связей более 5 абонентских пунктов срок выполнения пункта 3.4.1 увеличивается пропорционально количеству абонентских пунктов из расчета каждые 5 абонентских пунктов на 1 день.

## 4. Функции, права и обязанности администраторов и пользователей ЕЗСПД

4.1. Координатор.

4.1.1. Координатор назначается и отстраняется от исполнения возложенных функций приказом руководителя Оператора ЕЗСПД.

4.1.2. В случае смены сотрудника, на которого возложены функции Координатора, Оператор ЕЗСПД обязан в течение двух рабочих дней известить об этом Участников ЕЗСПД.

4.1.3. Координатор осуществляет:

общую стратегию развития ЕЗСПД;

определение перечня средств защиты информации, устанавливаемых на Абонентских пунктах;

согласование организаций, осуществляющих техническое обслуживание сегмента ЕЗСПД, имеющих соответствующие лицензии на работу и обслуживание средств криптографической защиты информации.

4.2. Главный администратор.

4.2.1. Главный администратор назначается и отстраняется от исполнения возложенных функций приказом руководителя Оператора ЕЗСПД.

4.2.2. В случае смены сотрудника, на которого возложены функции Главного администратора, Оператор ЕЗСПД обязан в течение двух рабочих дней известить об этом Участников ЕЗСПД.

4.2.3. Главный администратор обязан:

следить за работоспособностью центральной части ЕЗСПД;

оперативно решать все проблемы, возникающие в центральной части ЕЗСПД;

изготавливать ключевые файлы и передавать их согласно данному Регламенту;

оказывать Участникам ЕЗСПД методическую помощь в настройках криптосредств путем изготовления инструкций и пособий, размещаемых на информационных ресурсах Оператора ЕЗСПД;

оказывать методическую помощь Участникам ЕЗСПД в организационных вопросах, связанных с эксплуатацией средств криптографической защиты.

4.2.4. Главный администратор вправе отказать в помощи в настройке средств криптографической защиты Участника ЕЗСПД в случае возникновения неисправностей на участке ЕЗСПД, находящемся в ответственности Участника ЕЗСПД.

4.2.5. Главный администратор не осуществляет настройку и не несет ответственности за оборудования и программное обеспечение, принадлежащие Участнику ЕЗСПД.

4.3. Локальный администратор.

4.3.1. Исполнение функций Локального администратора возлагается на сотрудника Участника ЕЗСПД.

4.3.2. Локальный администратор назначается и отстраняется от исполнения возложенных функций приказом руководителя Участника ЕЗСПД.

4.3.3. Необходимым условием назначения Локального администратора является подписание с ним соглашения о неразглашении информации, полученной вследствие выполнения своих обязанностей.

4.3.4. В случае смены сотрудника, на которого возложены функции Локального администратора, Участник ЕЗСПД обязан в течение двух рабочих дней известить об этом Оператора ЕЗСПД.

4.3.5. Копию приказа о возложении функций Локального администратора на сотрудника Участника ЕЗСПД, а также копию подписанного с этим сотрудником соглашения о неразглашении информации, полученной вследствие выполнения своих обязанностей, передаются Участником ЕЗСПД Координатору.

4.3.6. На Локального администратора Участника ЕЗСПД возлагается ответственность за исправное функционирование ПО VipNet у Участника ЕЗСПД.

4.3.7. Участник ЕЗСПД для выполнения функций Локального администратора вправе привлекать на договорной основе организации,

имеющие соответствующие лицензии на работу и обслуживание средств криптографической защиты информации, по согласованию с Координатором.

4.3.8. На Локального администратора возлагается ответственность за последствия, вызванные перебоями в функционировании и/или неправильным функционированием ПО VipNet Участника ЕЗСПД.

4.3.9. Локальный администратор обязан:

знать структуру и состав своего сегмента ЕЗСПД;

следить за работоспособностью сегмента ЕЗСПД, находящегося в ответственности Участника ЕЗСПД;

оперативно решать все проблемы, возникающие в сегменте ЕЗСПД, находящемся в ответственности Участника ЕЗСПД;

обеспечивать подключение сегмента ЕЗСПД к центральной части ЕЗСПД по каналам связи, в том числе сети Интернет, в рабочее время;

заблаговременно оповещать Главного администратора о предстоящей плановой смене ключевой информации;

выполнять требования законодательства Российской Федерации и настоящего Регламента.

4.3.10. Локальный администратор вправе для выполнения части своих функций привлекать на договорной основе организации, имеющие соответствующие лицензии на работу и обслуживание средств криптографической защиты информации, по согласованию с Координатором.

4.3.11. Локальный администратор не вправе передавать Абонентские пункты для проведения ремонтно-восстановительных работ сторонним организациям, не имеющим соответствующих лицензий на работу и обслуживание средств криптографической защиты информации.

4.4. Абонент.

4.4.1. Исполнение функций Абонентов Участника ЕЗСПД возлагается на сотрудников Участника ЕЗСПД.

4.4.2. Абоненты назначаются и отстраняются от исполнения возложенных функций приказом руководителя Участника ЕЗСПД.

4.4.3. В случае смены сотрудника, на которого возложены функции Абонента, Участник ЕЗСПД обязан в течение двух рабочих дней известить об этом Оператора ЕЗСПД.

4.4.4. Абонент вправе:

использовать ЕЗСПД для подключения к Информационным системам Оператора и Участников ЕЗСПД в рамках своих функциональных обязанностей;

использовать ЕЗСПД для обмена служебной информацией

4.4.5. Абонент обязан:

обеспечивать подключение Абонентского пункта к ЕЗСПД в рабочее время;

заблаговременно оповещать Локального администратора о предстоящей плановой смене ключевой информации;

обеспечивать конфиденциальность пароля пользователя для авторизации в ЕЗСПД, а в случае нарушения его конфиденциальности – немедленно уведомлять Локального администратора.

4.4.6. Абонент не вправе:

предоставлять доступ к Абонентскому пункту сторонним лицам;

предоставлять удаленный доступ к Абонентскому пункту пользователям, не являющимся Абонентами ЕЗСПД;

вносить изменения в настройки, удалять и блокировать работу средств защиты информации, установленных на Абонентском пункте.

## 5. Функционирование ЕЗСПД

5.1. Обеспечение доступа к Информационным системам и защиты информации при передаче данных.

Для защиты от несанкционированного доступа к служебной информации и установленного ПО VipNet на абонентском пункте должны быть установлены средство защиты информации от НСД и антивирусная программа, сертифицированные ФСБ и ФСТЭК России, согласованные с Оператором ЕЗСПД.

5.2. Передача служебных сведений посредством ПО ViPNet «Деловая почта».

Посредством ПО ViPNet «Деловая почта» передается зашифрованная и заверенная электронной подписью служебная конфиденциальная цифровая информация между участниками защищенной сети.

5.3. Подтверждение достоверности и подлинности передаваемых сообщений.

Подтверждение достоверности, подлинности и авторства передаваемых сведений обеспечивается средствами электронной подписи, предоставляемой ПО ViPNet «Деловая почта», входящей в состав ПАК защиты информации ViPNet-Клиент, либо иных средств электронной подписи, используемых в соответствующих сегментах ЕЗСПД.

5.4. Обеспечение удаленного доступа к Абонентским пунктам.

Удаленный доступ к Абонентскому пункту предоставляется Абонентам средствами, интегрированными в ViPNet-Клиент. Удаленный доступ к Абонентскому пункту лицам, не являющимся Абонентами, предоставляется по согласованию с Координатором.

5.5. Плановая смена ключевой информации.

5.6. Плановая смена закрытого ключа проводится автоматически. Для этого абонентские пункты должны быть постоянно доступны в сети в течение рабочего времени, а координаторы круглосуточно.

Внеплановая смена ключевой информации.

Внеплановая смена ключевой информации производится в автоматическом режиме при компрометации ключей.

## 6. Компрометация ключей

6.1. 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.

6.2. 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.

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

6.4. 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.

6.5. Локальный администратор доводит информацию о факте компрометации (или предполагаемом факте компрометации) до Координатора или Главного администратора в течение одного рабочего дня.

6.6. Главный администратор при получении сообщения о компрометации ключевой информации в течение одного рабочего дня обязан:

в программном обеспечение 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 нескомпрометированных ключах из резервного набора персональных ключей, поэтому могут передаваться на скомпрометированный Абонентский пункт по любым каналам связи;

произвести рассылку или передать иным доверенным способом сформированных обновлений ключей на Абонентские пункты ЕЗСПД.

## 7. Организация межсетевого взаимодействия ЕЗСПД со сторонними сетями VipNet

7.1. Определение условий межсетевого взаимодействия ЕЗСПД со сторонней ViPNet-сетью.

7.1.1. Межсетевое защищенное информационное взаимодействие сторонней ViPNet-сети с ЕЗСПД организуется по технологии межсетевого взаимодействия ViPNet-сетей.

7.1.2. Передача данных между узлами ViPNet-сетей может осуществляться либо напрямую, либо через узлы одной из ViPNet-сетей.

7.1.3. Межсетевое защищенное информационное взаимодействие организуется с помощью индивидуального симметричного межсетевого мастер-ключа (ИСММК).

7.1.4. ИСММК формируют Главный администратор ЕЗСПД и администраторы сторонних ViPNet-сетей (далее – Администраторы сетей) для каждой из сетей, с которой должно осуществляться взаимодействие.

7.1.5. Администраторы сетей выделяют узлы своих сетей, которые будут участвовать в межсетевом взаимодействии. Выделенные узлы сетей будут связаны в ЦУСах взаимодействующих сетей, а также будут иметь ключи для шифрования и подтверждения достоверности и подлинности передаваемых данных.

7.1.6. Администраторы сетей выбирают устройства ViPNet-Координаторы, которые будут выполнять функции серверов-шлюзов при межсетевом взаимодействии сетей.

7.2. Порядок организации межсетевого защищенного информационного взаимодействия между ЕЗСПД и сторонней ViPNet-сетью.

7.2.1. Для организации межсетевого защищенного информационного взаимодействия между ЕЗСПД и сторонней ViPNet-сетью администратор сторонней ViPNet-сети направляет Оператору ЕЗСПД официальное информационное письмо, в котором информирует о необходимости организации межсетевого защищенного информационного взаимодействия между заданными ViPNet-сетями с обязательным указанием целей, причин и предполагаемых результатов подключения, а также узлов своей сети, шлюза и предполагаемых узлов ЕЗСПД. В течение пяти рабочих дней с момента получения официального информационного письма Оператор ЕЗСПД направляет официальный ответ с подтверждением или отказом от межсетевого защищенного информационного взаимодействия с указанием причин. При получении подтверждения о межсетевом защищенном взаимодействии организация, владеющая сторонней ViPNet-сетью, заключает с Оператором

ЕЗСПД соглашение о межсетевом взаимодействии, в соответствии с типовым соглашением (приложение № 7).

7.2.2. После заключения соглашения в течение пяти рабочих дней в Центре управления сетью (ЦУС) и Удостоверяющем ключевом центре (УКЦ) сторонней ViPNet-сети производится формирование необходимой адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая свои корневые сертификаты для каждой из сетей, с которой должно осуществляться взаимодействие.

7.2.3. Указанные данные (начальный экспорт) доверенным способом передаются в ЦУС ЕЗСПД.

7.2.4. В течение трех рабочих дней с момента получения начального экспорта в ЦУС и УКЦ ЕЗСПД производится ввод и обработка (импорт) полученных из ЦУС сторонней ViPNet-сети данных (начального экспорта), установление связей своих узлов с узлами ЦУС, предоставившего информацию. Далее в ЦУС ЕЗСПД создается ответная информация (ответный экспорт) для ЦУС, приславшего первичную информацию, включая свои корневые сертификаты.

7.2.5. В течение трех рабочих дней ответная информация (ответный экспорт) доверенным способом передается в ЦУС сторонней ViPNet-сети, создавшей начальный экспорт, где она обрабатывается и вводится в действие. На этом этапе завершается процесс создания межсетевого защищенного взаимодействия между ЦУС, и дальнейший обмен данными между ними производится в автоматическом режиме, а в случае невозможности – иным доверенным способом.

7.2.6. После рассылки каждым ЦУС сформированных обновлений ключевой и справочной информации на свои узлы, участвующие в межсетевом взаимодействии, между данными узлами различных сетей осуществляется защищенный обмен информацией.

7.2.7. После завершения процедуры организации межсетевого защищенного информационного взаимодействия подписывается протокол установления межсетевого взаимодействия (приложение № 7).

7.3. Порядок модификации межсетевого защищенного информационного взаимодействия между ViPNet-сетями при изменении состава узлов.

Порядок модификации межсетевого защищенного информационного взаимодействия между ViPNet-сетями предполагает выполнение следующих технологических и организационных мероприятий:

7.3.1. В процессе функционирования межсетевого защищенного информационного взаимодействия ViPNet-сетей в одной или нескольких сетях может потребоваться изменение состава узлов, участвующих в межсетевом защищенном взаимодействии, добавление или удаление сетевого узла, а также установление или удаление связей между существующими узлами.

7.3.2. При модификации межсетевого защищенного информационного взаимодействия в какой-либо ViPNet-сети администратор данной сети не позднее чем за пять рабочих дней направляет официальное информационное сообщение администратору другой ViPNet-сети с указанием предполагаемых изменений.

7.3.3. После получения официального ответа (в течение трех рабочих дней с момента получения официального информационного сообщения) с разрешением внесения изменений в структуру сети администратор сети в своем ЦУС производит соответствующие изменения в структуре связей своей сети, формирует экспортные данные и передает их в соответствующий ЦУС в автоматическом режиме, а в случае невозможности иным доверенным способом в течение трех рабочих дней с момента получения официального разрешения.

7.3.4. В ЦУС сети, которой касается данная модификация, в течение пяти рабочих дней с момента получения экспортных данных производится обработка (импорт) полученных данных. Далее в ЦУС создается ответная информация (ответный экспорт) для ЦУСа, приславшего первичную информацию.

7.3.5. Ответная информация передается в ЦУС сети, от которой поступила первичная информация, в автоматическом режиме по защищенному каналу связи либо иным доверенным способом, где она обрабатывается и вводится в действие в течение трех дней с момента получения. На этом завершается процесс модификации межсетевого защищенного взаимодействия между ЦУС ViPNet-сетей.

7.3.6. После рассылки каждым ЦУС сформированных обновлений ключевой и справочной информации на свои узлы, которых касается модификация, данные узлы продолжают или прекращают производить защищенный электронный документооборот при межсетевом взаимодействии.

7.4. Порядок модификации межсетевого защищенного информационного взаимодействия между ViPNet-сетями в случае плановой смены межсетевого мастер-ключа.

7.4.1. Перед тем, как осуществлять плановую смену межсетевого мастер-ключа, Администраторы сетей, для связи которых будет использоваться новый межсетевой мастер-ключ, должны согласовать следующие вопросы:

выбрать тип межсетевого мастер-ключа, который будет использоваться для связи между сетями;

если предполагается использовать симметричный мастер-ключ, то выбрать Администратора сети, который будет создавать новый межсетевой мастер-ключ;

выбрать и согласовать время проведения смены межсетевого мастер-ключа и последующего обновления ключей шифрования для узлов своих сетей.

7.4.2. Формирование нового межсетевого мастер-ключа.

Формирование нового межсетевого мастер-ключа производится в течение пяти рабочих дней с момента договоренности о плановой смене межсетевого мастер-ключа.

7.4.3. Процедура создания экспорта и приема импорта.

После смены межсетевого мастер-ключа производится процедура создания экспортных данных (не позднее трех рабочих дней с момента формирования нового межсетевого мастер-ключа) и приема импортных данных (не позднее трех рабочих дней с момента получения экспортных данных).

7.4.4. Межсетевое взаимодействие после смены межсетевого мастер-ключа.

Связь между сетевыми узлами взаимодействующих ViPNet-сетей после смены межсетевого мастер-ключа возможна только после прохождения обновлений ключевой информации на всех соответствующих сетевых узлах данных сетей.

7.5. Порядок организации межсетевого защищенного информационного взаимодействия между ViPNet-сетями сторон в случае компрометации ключей.

Администратор сети в случае компрометации ключей пользователя своей сети в ЦУС и УКЦ своей сети проводит процедуру внеплановой компрометации ключей данного пользователя, которая предполагает выполнение следующих технологических и организационных мероприятий в течение трех рабочих дней с момента получения данных о компрометации ключа:

7.5.1. Администратор сети оповещает о факте компрометации ключей всех пользователей, связанных со скомпрометированным пользователем. После получения данного сообщения пользователи не должны использовать скомпрометированные ключи.

7.5.2. Администратор сети объявляет ключи данного пользователя скомпрометированными, создает и отправляет экспорт адресно-ключевой информации в сети, с пользователями которых был связан скомпрометированный пользователь.

7.5.3. Администратор сети создает и отправляет (либо передает доверенным способом) новую ключевую информацию как для скомпрометированного пользователя, так и для всех пользователей своей сети, с которыми он был связан.

7.5.4. В течение четырех рабочих дней после приема и обработки импорта переданных данных Администратор сети, пользователи которой взаимодействовали с пользователем, ключи которого скомпрометированы, создает новую ключевую информацию своим пользователям.

7.5.5. После прохождения обновления новой ключевой информации на всех взаимодействующих узлах ViPNet-сетей пользователи данных узлов могут продолжать производить защищенный обмен информацией.

7.6. Внеплановая смена межсетевого мастер-ключа.

Внеплановая смена ключей выполняется в случае компрометации или угрозы компрометации межсетевого мастер-ключа, на котором происходит организация межсетевого защищенного информационного взаимодействия между ViPNet-сетями.

7.6.1. В случае компрометации симметричного межсетевого мастер-ключа считается скомпрометированной вся ключевая информация, которая используется при межсетевом взаимодействии ViPNet-сетей, о чем в течение одного рабочего дня направляется официальное информационное сообщение другой Стороне.

7.6.2. Должно быть немедленно остановлено межсетевое защищенное информационное взаимодействие между ViPNet-сетями.

7.6.3. Для восстановления работы межсетевого защищенного информационного взаимодействия между ViPNet-сетями сторон необходимо провести технологические и организационные мероприятия, описанные в пункте 7.4.

## 8. Порядок разрешения конфликтных ситуаций

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

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

8.3. В случае необходимости для разрешения конфликтных ситуаций могут быть привлечены Координатор и Главный администратор.

Приложение № 1
к Регламенту функционирования единой защищенной сети передачи данных органов государственной власти Кабардино-Балкарской Республики и органов местного самоуправления

Управляющему делами
Главы и Правительства
Кабардино-Балкарской Республики

З.А. КАЛОВУ

Прошу подключить _____
(наименование организации)
к единой защищенной сети передачи данных Кабардино-Балкарской Республики.

Число подключаемых абонентских пунктов – ___ *(_____).*

Перечень информационных систем, к которым необходим доступ: _____.

Лицо, ответственное за подключение, контактный телефон: _____
_____.
(фамилия, имя, отчество, должность, телефон, e-mail)

Подробная схема сети _____
и копия договора _____ прилагается.

Руководитель организации _____ И.Фамилия

М.П.

Приложение № 2
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

# П Р И К А З

«___» _____2010 г. №____

О назначении Локального администратора сети

_____
(наименование организации)

Для осуществления мер по пресечению несанкционированного доступа, администрирования и обеспечения бесперебойной работы информационных систем и абонентских пунктов, принадлежащих _____ (наименование организации) и относящихся к Единой защищённой сети передачи данных Кабардино-Балкарской Республики

ПРИКАЗЫВАЮ:

1. Назначить Локальным администратором _____:
(наименование организации)

_____.
(фамилия, имя, отчество, должность)

2. В своей работе по выполнению функций Локального администратора _____ руководствоваться:
(наименование организации)

- действующим законодательством Российской Федерации;
- Регламентом Единой защищённой сети передачи данных Кабардино-Балкарской Республики.

3. Контроль за исполнением приказа _____.

Руководитель _____ И.Фамилия

Приложение № 3
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

П Р И К А З

«___» _____2010 г. №____

О назначении Абонентов ЕЗСПД КБР

_____
(наименование организации)

Для выполнения служебных обязанностей с использованием сервисов и информационных систем Единой защищённой сети передачи данных Кабардино-Балкарской Республики (далее – ЕЗСПД КБР)

ПРИКАЗЫВАЮ:

1. Назначить Абонентами ЕЗСПД КБР:

_____.
(фамилия, имя, отчество, должность)

2. В своей работе Абонентам ЕЗСПД КБР руководствоваться:

- действующим законодательством Российской Федерации;
- Регламентом Единой защищённой сети передачи данных Кабардино-Балкарской Республики.

3. Контроль за исполнением приказа _____.

Руководитель _____ И.Фамилия

Приложение 4
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

**Соглашение**
**о неразглашении персональных данных субъекта**

Я, _____, понимаю, что получаю доступ к персональным
(фамилия, имя, отчество)
данным третьих лиц.

Я понимаю, что получаю доступ к персональным данным граждан РФ. Я также понимаю, что во время исполнения своих обязанностей я занимаюсь сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб гражданину РФ, как прямой, так и косвенный.

Я подтверждаю, что не имею права разглашать сведения о (об):

анкетных и биографических данных;

образовании;

трудовом и общем стаже;

составе семьи;

паспортных данных;

воинском учете;

заработной плате;

социальных льготах;

специальности;

занимаемой должности;

наличии судимостей;

адресе места жительства, домашнем телефоне;

месте работы или учебы членов семьи и родственников;

содержании трудового договора;

составе декларируемых сведений о наличии материальных ценностей;

содержании декларации, подаваемой в налоговую инспекцию;

подлинниках и копиях приказов по личному составу;

личных делах и трудовых книжках;

делах, содержащих материалы по повышению квалификации и переподготовке, их аттестации, служебным расследованиям;

копиях отчетов, направляемых в органы статистики.

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работника, или их утраты я несу ответственность в соответствии со ст. 90 ТК РФ.

_____ _____
(должность) (Ф.И.О.)

"___"_____20____ г.

_____
(подпись)

Приложение № 5
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

# ДОВЕРЕННОСТЬ
на получение дистрибутива ключей

Я, _____, действующий на
(должность, фамилия, имя, отчество)
основании _____,
(основные реквизиты (наименование, номер и дата выдачи) документа, подтверждающего право лица, выступающего от имени организации, обращаться с заявлением)
доверяю _____,
(фамилия, имя, отчество)
_____,
(должность, структурное подразделение)
паспорт_____,
(серия, номер, дата выдачи, выдавшая организация)
получить в Управлении делами Главы и Правительства КБР дистрибутив ключей для первичного запуска прикладной программы ViPNet-сети №1465.

Подпись лица, получившего доверенность: _____
(фамилия, имя, отчество)

УДОСТОВЕРЯЮ:
_____
(должность, наименование организации)

Подпись: _____
(фамилия, имя, отчество)

М.П.

«____» _____ 20____ г.

Приложение № 6
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

Управляющему делами
Главы и Правительства
Кабардино-Балкарской Республики

З.А. КАЛОВУ

ЗАЯВКА
на изменение направлений связи и/или предоставления доступа
к информационным системам ЕЗСПД КБР

| | | | |
|---|---|---|---|
| 1. Полное наименование организации без сокращений (на основании учредительных документов) | | | |
| | | | |
| 2. Сокращённое наименование организации | | | |
| | | | |
| 3. Направления связи для организации защищённого обмена информацией: | | | |
| | | | |
| 4. Перечень информационных систем, к которым необходим доступ: | | | |
| | | | |
| 5. Контактный телефон Локального администратора | | | |
| | | | |
| 6. Контактный e-mail Локального администратора | | | |
| | | | |
| *Дата заполнения заявки* | | *Подпись руководителя* | *М.П.* |

Приложение № 7
к Регламенту функционирования единой
защищенной сети передачи данных органов
государственной власти Кабардино-Балкарской
Республики и органов местного самоуправления

# СОГЛАШЕНИЕ О МЕЖСЕТЕВОМ ВЗАИМОДЕЙСТВИИ

г. Нальчик ___ _____ 20__ г.

Управление делами Главы и Правительства Кабардино-Балкарской Республики, именуемое в дальнейшем «Организация», в лице управляющего делами Калова Замира Ауесовича, действующего на основании Положения об Управлении делами Главы и Правительства Кабардино-Балкарской Республики, с одной стороны, и _____, именуемое в дальнейшем _____ *(краткое наименование организации),* в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

## 1. Предмет Соглашения

1.1. Целью Соглашения является обеспечение защищенного информационного взаимодействия при оказании государственных услуг абонентами защищенной ViPNet-сети Организации и абонентами защищенной ViPNet-сети _____ *(краткое наименование организации)*.

1.2. Предметом Соглашения является установление защищенного межсетевого взаимодействия защищенных ViPNet-сетей.

1.3. Межсетевое взаимодействие устанавливается между сетями:

| Номер сети | Наименование организации - администратора сети |
|---|---|
| № 1465 | Управление делами Главы и Правительства КБР |
| № _____ | |

1.4. Взаимодействие Сторон осуществляется на безвозмездной основе.

## 2. Права и обязанности Сторон

2.1. Организация:

2.1.1. Осуществляет администрирование защищенной ViPNet-сетью № 1465.

2.1.2. Обеспечивает работоспособность аппаратных, программных и телекоммуникационных средств, необходимых для функционирования администрируемой защищенной ViPNet-сети № 1465.

2.1.3. Обеспечивает в соответствии с законодательством Российской Федерации конфиденциальность информации, передаваемой между защищенными ViPNet-сетями Организации и _____ *(краткое наименование организации)*.

2.1.4. Определяет работников (сотрудников), ответственных за взаимодействие в рамках настоящего Соглашения (далее - уполномоченные лица), и сообщает _____ *(краткое наименование организации)* об определении таких уполномоченных лиц с указанием их контактных данных. Информирует _____*(краткое наименование организации)* об изменении указанных сведений.

2.2. _____ *(краткое наименование организации)*:

2.2.1. Осуществляет администрирование защищенной ViPNet-сети № ____.

2.2.2. Обеспечивает работоспособность аппаратных, программных и телекоммуникационных средств, необходимых для функционирования администрируемой защищенной ViPNet-сети № ____.

2.2.3. Обеспечивает в соответствии с законодательством Российской Федерации конфиденциальность информации, передаваемой между защищенными ViPNet-сетями _____ *(краткое наименование организации)* и Организации.

2.2.4. Определяет работников (сотрудников), ответственных за взаимодействие в рамках настоящего Соглашения (далее - уполномоченные лица), и сообщает Организации об определении таких уполномоченных лиц с указанием их контактных данных. Информирует Организацию об изменении указанных сведений.

## 3. Организация межсетевого взаимодействия

3.1. Для организации межсетевого взаимодействия, администраторы ViPNet-сетей Сторон производят формирование адресной и ключевой информации – формирование начального экспорта (индивидуальные симметричные межсетевые мастер-ключи связи и шифрования, справочная информация), включая корневые сертификаты для каждой ViPNet-сети.

3.2. Указанные данные (начальный экспорт) доверенным способом передаются в соответствующие центры управления ViPNet-сетей (ЦУС – аппаратные или программные средства для мониторинга, конфигурирования и управления узлами защищённой сети), с которыми должно осуществляться межсетевое взаимодействие.

3.3. В ЦУС 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 сертификаты.

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

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

3.6. После завершения процедуры организации межсетевого взаимодействия между ViPNet-сетями Сторон подписывается протокол установления межсетевого взаимодействия по форме приложения № 1 к настоящему Соглашению.

## 4. Ответственность Сторон

4.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению Стороны несут ответственность в соответствии с законодательством Российской Федерации.

4.1. Организация не несет ответственности за содержание информации, передаваемой между абонентами VipNet-сетей Организации и _____ *(краткое наименование организации)*.

## 5. Срок действия Соглашения

5.1. Настоящее Соглашение вступает в силу с момента его подписания и действует до 31 декабря 2016 г.

5.2. Настоящее Соглашение может быть расторгнуто по соглашению Сторон или в одностороннем порядке по инициативе одной из Сторон, которая письменно уведомляет о расторжении другую Сторону не позднее чем за 30 (тридцать) дней до даты расторжения Соглашения.

5.3. При отсутствии заявления одной из Сторон о расторжении Соглашение продлевается (пролонгируется) на следующий календарный год.

## 6. Заключительные положения

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

6.2. Все изменения и дополнения к настоящему Соглашению оформляются в письменной форме и являются его неотъемлемой частью.

## 7. Реквизиты и подписи Сторон

| | |
|---|---|
| | Управление делами Главы и Правительства Кабардино-Балкарской Республики<br><br>360028, г. Нальчик, пр. Ленина, 27<br>ИНН 0721021159<br>КПП 072501001<br>тел. (8662)40-67-87,<br>e-mail: ud@kbr.ru |
| Руководитель | Управляющий делами Главы и Правительства Кабардино-Балкарской Республики |
| _____ | _____ З. Калов |
| М.П. | М.П. |

Приложение
к Соглашению о межсетевом
взаимодействии
от ____ _____ 20__ г.

# ПРОТОКОЛ
## установления межсетевого взаимодействия

«____» _____ 20___ г.

1. Межсетевое взаимодействие устанавливается между сетями:

| Номер сети | Наименование организации |
|---|---|
| № 1465 | Управление делами Главы и Правительства Кабардино-Балкарской Республики<br>(полное наименование организации) |
| № _____ | _____<br>(полное наименование организации) |

2. Процедуру установления межсетевого взаимодействия осуществляли:

| Номер сети | Должность | Ф.И.О. |
|---|---|---|
| № 1465 | эксперт отдела ТЗИ | |
| № _____ | | |

3. Передача начального и ответного экспорта между сетями № 1465 и № _____ осуществлялась через специалиста, уполномоченного Сторонами на данные действия.

4. Для установления межсетевого взаимодействия использовался индивидуальный симметричный межсетевой мастер-ключ, созданный в сети № 1465 .

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

в сети № 1465 _____ – «_____»,

в сети № ____ _____ – «_____».

6. При установлении межсетевого взаимодействия в части ЭП были произведены импорты справочников ЭП главных абонентов сети № 1465 и сети № _____.

7. Смена межсетевых ключей, изменение состава Абонентных пунктов, участвующих в межсетевом взаимодействии, производится после предварительного согласования средствами взаимного экспорта/импорта, о чем администраторы защищенных сетей уведомляют друг друга с помощью ПО ViPNet [Клиент] [Деловая почта] с указанием производимых изменений.

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

Руководитель

_____

Управляющий делами Главы и Правительства
Кабардино-Балкарской Республики

_____ З. Калов

Администратор безопасности ViPNet-сети № ____

_____ _____
*(Ф.И.О.)* *(подпись)*

*“____” _____ 20___ г.*

*М.П.*

Администратор безопасности ViPNet-сети № 1465

_____ _____
*(Ф.И.О.)* *(подпись)*

*“____” _____ 20___ г.*

*М.П.*