УТВЕРЖДАЮ
Руководитель ГБУ «Центр информационных технологий Амурской области»

_____С.В. Щербаков

«01» 11 2016 г.

РЕГЛАМЕНТ

взаимодействия участников защищенной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области»

1. Термины и определения.

В настоящей Политике используются следующие понятия:

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].

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

Компрометация ключей - факт доступа постороннего лица к защищаемой информации, а также подозрение на данный факт.

Защищенная сеть - защищенная виртуальная сеть государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области», построенная по технологии ViPNet.

Претендент - организация, имеющая намерения подключиться к Защищенной сети.

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

Оператор - государственное бюджетное учреждение Амурской области «Центр информационных технологий Амурской области».

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

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

Главный администратор - сотрудник Оператора, осуществляющий общую политику администрирования всей Защищенной сети.

2. Общие положения.

2.1 Регламент взаимодействия участников защищенной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области» (далее - 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 июня 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».

2.2 Регламент определяет и устанавливает:

- порядок подключения Участников к Защищенной сети;
- порядок предоставления Участникам доступа к информационным ресурсам Защищенной сети;
- порядок организации защищенного межсетевого взаимодействия;
- порядок действий при компрометации ключей;
- порядок разрешения конфликтных ситуаций.

3. Порядок подключения Участников к Защищенной сети.

3.1. Подключение Участников к Защищенной сети включает в себя следующие стадии:

- заявительная стадия;
- стадия рассмотрения заявления;
- приобретение программного обеспечения;
- формирование и передача ключевой информации.

3.2. Заявительная стадия.

Претендент направляет в адрес Оператора заявление о намерении подключиться к Защищенной сети (Приложение № 1).

В заявлении должна содержаться следующая информация:

- предполагаемое количество подключаемых Абонентских пунктов;
- общий перечень Участников, с которыми необходима организация защищенного обмена;
- перечень информационных ресурсов Защищенной сети, к которым необходимо организовать доступ;
- ФИО и контактный телефон лица, ответственного за подключение Претендента.

3.3. Стадия рассмотрения заявления.

3.3.1. Оператор в течение 5-ти рабочих дней со дня получения заявления о намерении подключиться к Защищенной сети, проводит оценку оснований для подключения Претендента к Защищенной сети, технической возможности организации связей и доступа к информационным ресурсам.

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

3.3.3. Решение о подключении Претендента к Защищенной сети, направляется в письменной форме в адрес Претендента в течение 3-х рабочих дней со дня принятия указанного решения.

3.3.4. Оператор имеет право отказать Претенденту в подключении к Защищенной сети, объяснив причину отказа. Решение об отказе в подключении Претендента к Защищенной сети направляется в письменной форме в адрес Претендента в течение 3-х рабочих дней со дня принятия указанного решения.

3.4. Приобретение программного обеспечения ViPNet [Клиент] Претендентом.

3.4.1. В случае принятия положительного решения о подключении к Защищенной сети, Претендент приобретает программное обеспечение ViPNet [Клиент] с указанием номера Защищенной сети для подключения - 2102.

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

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

3.5. Формирование и передача ключевой информации.

3.5.1. Претендент, после получения информации о поступлении регистрационных файлов, формирует и направляет в адрес Оператора заявление на подключение (Приложение № 2), а также заявления на создание ключевого дистрибутива и сертификата ключа проверки электронной подписи (Приложение № 3) в количестве приобретенных лицензий на программное обеспечение ViPNet [Клиент].

В случае необходимости организации доступа к информационным ресурсам Защищенной сети, Претендент также формирует и направляет в адрес Оператора заявление на предоставление доступа к информационным ресурсам (Приложение № 4).

3.5.2. В течение 2-х рабочих дней со дня получения от Претендента заявки на подключение Оператор:

- 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.

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

а) Предоставить в адрес Оператора копию приказа о назначении Администратора (Приложение № 5);

б) Направить к Оператору Администратора защищенной сети с доверенностью на получение ключевого дистрибутива (Приложение № 6).

3.5.4. После получения ключевых дистрибутивов Претендент считается Участником.

3.5.5. Факт выдачи ключевого дистрибутива заносится в Журнал учета выдачи ключевых дистрибутивов (Приложение № 7).

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

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

- заявительная стадия;
- стадия рассмотрения заявления;
- формирование и передача ключевой информации.

4.2. Заявительная стадия.

Участник, желающий изменить направление связей и/или получить доступ к информационным ресурсам Защищенной сети, направляет в адрес Оператора заявление за подписью руководителя (Приложение №8).

4.3. Стадия рассмотрения заявления.

4.3.1. Оператор в течение 2-х рабочих дней со дня получения рассматривает заявление, проводит оценку технической возможности для изменения направлений связи и/или организации доступа к информационным ресурсам Защищенной сети.

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

4.4. Формирование и передача ключевой информации.

4.4.1. В течение 3-х рабочих дней со дня принятия решения об изменении направлений связи и/или организации доступа к информационным ресурсам Защищенной сети Оператор:

- 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 посредством электронной почты.

4.4.2. Новая справочная и ключевая информация при поступлении на Абонентский пункт автоматически обновляет существующую справочную и ключевую информацию.

5. Организация межсетевого взаимодействия с другими сетями ViPNet.

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

- заявительная стадия;
- стадия рассмотрения заявления;
- организация межсетевого взаимодействия, формирование и передача ключевой информации.

5.2. Заявительная стадия.

Для организации межсетевого взаимодействия между Участником и организацией, подключенной к сторонней сети ViPNet (далее – Организация), Участник или Организация готовят информационное письмо, в котором информируют Оператора о необходимости организации информационного межсетевого взаимодействия с указанием контактов лиц ответственных за организацию межсетевого взаимодействия.

5.3. Стадия рассмотрения заявления.

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

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

5.3.3. После принятия решения об организации межсетевого взаимодействия либо об отказе в организации Оператор в письменной форме уведомляет о принятом решении организацию, инициирующую данное взаимодействие.

5.4. Организация межсетевого взаимодействия, формирование и передача ключевой информации.

5.4.1. После принятия решения об установлении межсетевого взаимодействия Организация и Оператор, руководствуясь технической документацией, согласовывают и реализовывают индивидуальный проект организации межсетевого взаимодействия сетей ViPNet.

5.4.2. После установления межсетевого взаимодействия Участник, желающий изменить направление связей и/или получить доступ к информационным ресурсам Защищенной сети Организации, направляет в адрес Оператор заявление за подписью руководителя (Приложение №8).

5.4.3. В течение 2-х рабочих дней со дня получения заявления об изменении направлений связи и/или организации доступа к информационным ресурсам Защищенной сети Оператор:

- 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 посредством электронной почты.

5.4.4. Новая справочная и ключевая информация при поступлении на Абонентский пункт автоматически обновляет существующую справочную и ключевую информацию.

6. Порядок действий при компрометации 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) съемный носитель ключевой информации Абонента;

- посторонние лица могли получить неконтролируемый физический доступ к ключевой информации, хранящейся на Абонентском пункте;

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 ее передаче посредством Защищенной сети.

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 Администратору.

6.5. Администратор доводит информацию о факте компрометации до Главного администратора.

6.6. Главный администратор при получении сообщения о компрометации ключевой информации в течение 1-го рабочего дня должен:

- 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 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.

7. Порядок разрешения конфликтных ситуаций.

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

7.2. Разрешение конфликтных ситуаций осуществляется путем взаимодействия Администраторов Участников, у которых возникли претензии.

7.3. В случае необходимости, для разрешения конфликтных ситуаций может быть привлечен Главный администратор.

7.4. Данный Регламент описывает только порядок взаимодействия Участников и не рассматривает иные вопросы.

Приложение № 1
к Регламенту

Руководителю
ГБУ «Центр информационных технологий
Амурской области»
Щербакову С.В.

О подключении
к защищенной виртуальной сети ViPNet
государственного бюджетного учреждения
Амурской области «Центр информационных
технологий Амурской области»

Прошу подключить _____ к защищенной виртуальной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области» для обмена информацией с _____.

Предполагаемое число подключаемых Абонентских пунктов – ___.

Лицо, ответственное за подключение, контактный телефон и адрес электронной почты: _____.

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

М.П.

Приложение № 2
к Регламенту

Руководителю
ГБУ «Центр информационных технологий
Амурской области»
Щербакову С.В.

ЗАЯВЛЕНИЕ
на подключение к защищенной виртуальной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области»

1. Полное наименование организации
2. Сокращенное название организации
3. Юридический адрес организации
4. Количество необходимых для регистрации Абонентских пунктов
5. Наименование Абонентских пунктов (не более 47 символов включая пробелы)
1 – Наименование АП №1 2 – Наименование АП №2 …
6. ФИО Администратора
7. Контактный телефон, E-mail Администратора
8. Направления связи для организации защищенного обмена информацией (если требуется):
Участник Защищенной сети 1 Участник Защищенной сети 2 …
9. Перечень информационных ресурсов Защищенной сети, к которым необходим доступ (если требуется):
ИР 1 ИР 2 …

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

Приложение № 3
к Регламенту

Руководителю
ГБУ «Центр информационных технологий
Амурской области»
Щербакову С.В.

ЗАЯВЛЕНИЕ
на создание ключевого дистрибутива и сертификата ключа проверки электронной подписи

1. Полное наименование организации	
2. Наименование Абонентского пункта	
3. Регистрационные данные для выпуска сертификата	
Общее Имя (ФИО)	
Должность	
Подразделение	
Организация	
Населенный пункт	
Область	Амурская область
Страна	RU
Адрес эл. почты	

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

Приложение № 4
к Регламенту

Руководителю
ГБУ «Центр информационных технологий
Амурской области»
Щербакову С.В.

ЗАЯВЛЕНИЕ
на предоставление доступа к информационным ресурсам

1. Полное наименование организации
2. Наименование Абонентских пунктов (идентификаторы узлов)
1 – Наименование АП №1 (0x000000) 2 – Наименование АП №2 (0x000000) …
3. IP-адрес (указывается только в случае если узел является Координатором)
4. Перечень информационных ресурсов Защищенной сети, к которым необходим доступ
ИР 1 ИР 2 …
5. IP-адреса информационных ресурсов Защищенной сети, к которым необходим доступ
ИР 1 – 10.x.x.x ИР 2 – 10.x.x.x …
6. Перечень протоколов и портов, по которым необходим доступ
ICMP, TCP (80, 443) , UDP (5222)
7. Изменение доступа (добавить, удалить)

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

Приложение № 5
к Регламенту

ПРИКАЗ

«___» _____ 201_ 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 государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области»

ПРИКАЗЫВАЮ:

1. Назначить Администратором защищенной сети:

- ФИО – должность.

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

- Регламентом взаимодействия участников защищенной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области».

3. Контроль за исполнением приказа _____.

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

М.П.

Приложение № 6
к Регламенту

Доверенность
на получение ключевого дистрибутива

(наименование населенного пункта) «__»_____201_ г.

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

(фамилия, имя, отчество), (серия и номер паспорта, кем и когда выдан) получить в государственном бюджетном учреждении Амурской области «Центр информационных технологий Амурской области» ключевой дистрибутив для первичного запуска прикладной программного обеспечения ViPNet [Клиент].

Настоящая доверенность действительна по «___» _____ 201__г.

Подпись уполномоченного представителя _____/_____
(подпись доверенного лица) (ФИО)

удостоверяю.

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

М.П.

Приложение № 7
к Регламенту

Журнал учета выдачи ключевых дистрибутивов

№ п/п	Идентификатор дистрибутива	Наименование СКЗИ	Отметка о выдаче		Отметка о получении	
			От кого получены (Ф.И.О. сотрудника)	Дата	Ф.И.О.	Дата
1.		Ключевой дистрибутив				
2.		Ключевой дистрибутив				
3.		Ключевой дистрибутив				
4.		Ключевой дистрибутив				
5.		Ключевой дистрибутив				
6.		Ключевой дистрибутив				
7.		Ключевой дистрибутив				

Приложение № 8
к Регламенту

Руководителю
ГБУ «Центр информационных технологий
Амурской области»
Щербакову С.В.

ЗАЯВЛЕНИЕ
на изменение направлений связи Защищенной виртуальной сети ViPNet государственного бюджетного учреждения Амурской области «Центр информационных технологий Амурской области»

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)

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