

## **ТЕХНИЧЕСКИЕ УСЛОВИЯ**

подключения автоматизированных рабочих мест пользователей к защищенной сети для функционирования системы личного приема граждан на базе специального программного обеспечения по проведению личного приема и приема в режиме видео-конференц-связи, видеосвязи, аудиосвязи и иных видов связи

## СОДЕРЖАНИЕ

<b>СПИСОК ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ.....</b>	<b>3</b>
<b>ВВЕДЕНИЕ.....</b>	<b>4</b>
<b>1. ОБЩИЕ ПОЛОЖЕНИЯ.....</b>	<b>5</b>
1.1. ОПИСАНИЕ ЗС ОДПГ.....	5
<b>2. РЕГЛАМЕНТ ДЕЙСТВИЙ ОТВЕТСТВЕННОГО ЛИЦА ПРИ ПОДКЛЮЧЕНИИ АРМ ПОЛЬЗОВАТЕЛЕЙ К ЗАЩИЩЁННОЙ СЕТИ ДЛЯ ОБЕСПЕЧЕНИЯ ПРОВЕДЕНИЯ ЕЖЕГОДНОГО ОБЩЕРОССИЙСКОГО ДНЯ ПРИЕМА ГРАЖДАН И ЕЖЕДНЕВНОЙ РАБОТЫ ПО РЕЗУЛЬТАТАМ РАССМОТРЕНИЯ ОБРАЩЕНИЙ .....</b>	<b>6</b>
2.1. ОБЩИЕ СВЕДЕНИЯ .....	6
2.2. ПЕРЕЧЕНЬ МЕРОПРИЯТИЙ ПО ПОДКЛЮЧЕНИЮ АРМ ПОЛЬЗОВАТЕЛЕЙ.....	8
2.3. ЭКСПЛУАТАЦИЯ АРМ ПОЛЬЗОВАТЕЛЕЙ .....	10
2.4. ТЕХНИЧЕСКОЕ СОПРОВОЖДЕНИЕ ПО VIPNET CLIENT .....	10
<b>3. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ПОДКЛЮЧЕНИЮ АРМ ПОЛЬЗОВАТЕЛЕЙ К ЗС ОДПГ .....</b>	<b>11</b>
3.1. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПОДКЛЮЧЕНИЯ К ЗС ОДПГ .....	11
3.2. ТРЕБОВАНИЯ К АРМ ПОЛЬЗОВАТЕЛЯ.....	14
3.3. ТРЕБОВАНИЯ К КАНАЛАМ СВЯЗИ .....	15
3.4. ОРГАНИЗАЦИОННЫЕ ТРЕБОВАНИЯ .....	15

**СПИСОК ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ**

NAT	англ. Network Address Translation, преобразование сетевых адресов
UDP	англ. User Datagram Protocol, протокол пользовательских датаграмм
VPN	англ. Virtual Private Network, виртуальная частная сеть
АРМ	Автоматизированное рабочее место
ЗС	Защищенная сеть
ОДПГ	Обеспечение проведения ежегодного общероссийского дня приема граждан и ежедневной работы по результатам рассмотрения обращений
ОС	Операционная система
СКЗИ	Средство криптографической защиты информации
ПО	Программное обеспечение
ИБ	Информационная безопасность
ФСБ России	Федеральная служба безопасности Российской Федерации

## **ВВЕДЕНИЕ**

Настоящие технические условия определяют требования к подключению автоматизированного рабочего места (далее – АРМ) пользователя к защищенной сети (далее – ЗС) для обеспечения проведения ежегодного общероссийского дня приема граждан и ежедневной работы по результатам рассмотрения обращений (далее – ОДПГ).

Данный документ предназначен для пользователей, имеющих квалификацию системного администратора (технического специалиста), обладающего знаниями и опытом в области конфигурирования, эксплуатации и управления персональным компьютером и сетевым оборудованием, а также знаниями в области информационной безопасности.

## **1. Общие положения**

### **1.1. Описание ЗС ОДПГ**

- 1.1.1. ЗС ОДПГ является мультисервисной системой информационного обмена аудио, видеоинформацией и электронными данными в реальном режиме времени.
- 1.1.2. ЗС ОДПГ обрабатывает обращения граждан, организаций и общественных объединений в государственные органы и органы местного самоуправления.
- 1.1.3. ЗС ОДПГ состоит из сети центрального узла связи, а также региональных сетей.
- 1.1.4. Защита данных ЗС ОДПГ, передаваемых по каналам сети связи общего пользования, обеспечивается применением технологии виртуальной частной сети (далее – VPN-сети), реализованной с помощью сертифицированных ФСБ России средств защиты ViPNet.
- 1.1.5. Каждая региональная VPN-сеть имеет собственный узел управления, который состоит из:
  - автоматизированного рабочего места (далее – АРМ) на базе программного комплекса (далее – ПК) ViPNet Administrator, обеспечивающего конфигурирование VPN-сети и подключение АРМ пользователя к ЗС ОДПГ;
  - криптошлюза - программно-аппаратного комплекса ViPNet Coordinator HW1000/2000, обеспечивающего защиту каналов связи.

## **2. Регламент действий ответственного лица при подключении АРМ пользователей к защищённой сети для обеспечения проведения ежегодного общероссийского дня приема граждан и ежедневной работы по результатам рассмотрения обращений**

В настоящем документе описывается порядок действий ответственного лица при подключении автоматизированных рабочих мест (далее – АРМ) пользователей органа государственной власти или органа местного самоуправления к защищённой сети (далее – ЗС) для обеспечения проведения ежегодного общероссийского дня приема граждан и ежедневной работы по результатам рассмотрения обращений (далее – ОДПГ).

### **2.1. Общие сведения**

ЗС ОДПГ состоит из VPN-сети центрального узла, а также региональных VPN-сетей.

Каждая региональная VPN-сеть имеет собственный узел управления, который состоит из:

– АРМ администратора на базе программного обеспечения (далее – ПО) ViPNet Administrator, обеспечивающего конфигурирование VPN-сети и подключение АРМ пользователей к ЗС ОДПГ;

– криптошлюза в виде программно-аппаратного комплекса (далее – ПАК) ViPNet Coordinator HW1000/2000, обеспечивающего защиту каналов связи.

Подключение АРМ пользователей региональной VPN-сети (далее – АРМ пользователей) к ресурсам ЗС ОДПГ осуществляется с использованием ПО ViPNet Client.

Типовая схема ЗС ОДПГ представлена на рисунке 1.

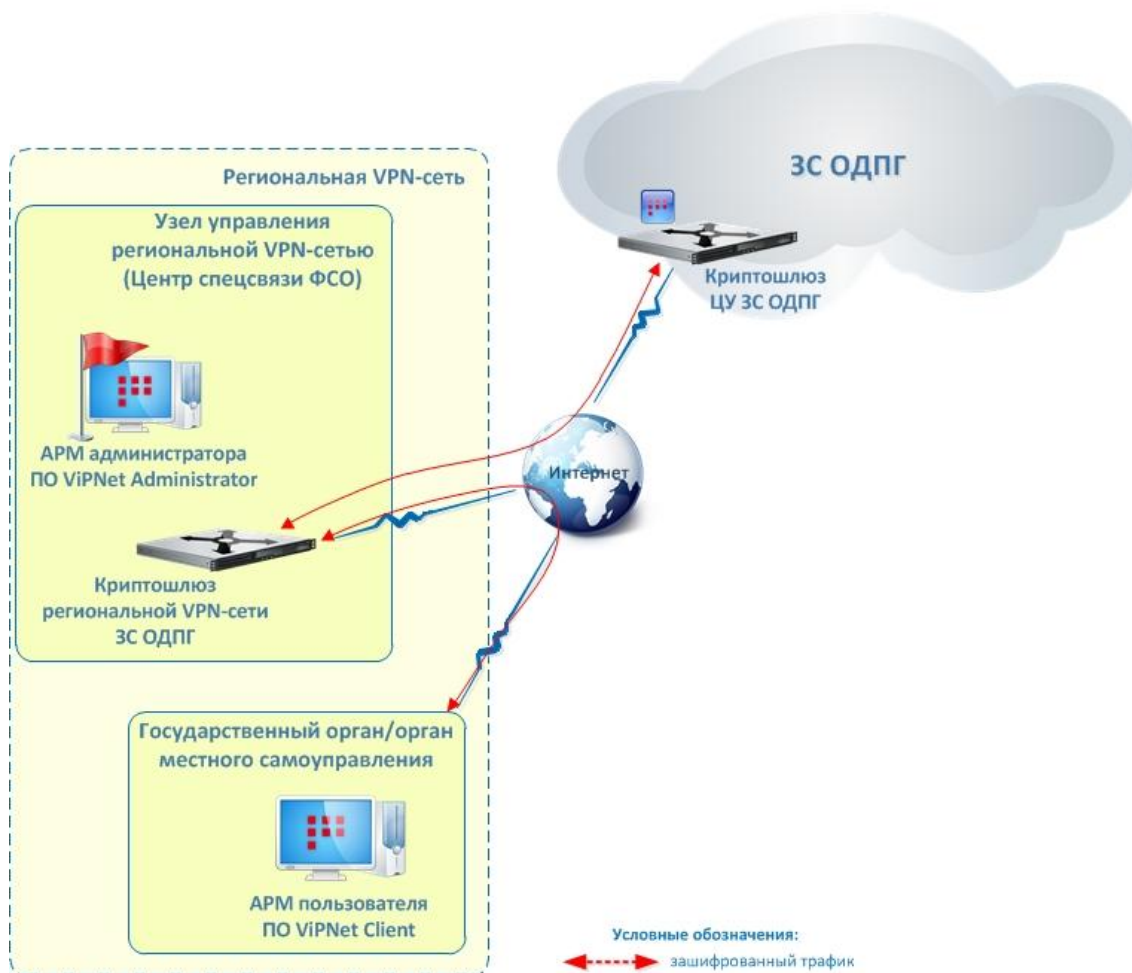


Рисунок 1. Типовая схема региональной VPN-сети

Узлы управления региональными VPN-сетями находятся в ведении региональных центров Федеральной службы охраны Российской Федерации (далее – ФСО России).

Управление региональной VPN-сетью осуществляется администратором данной сети.

Процесс подключения АРМ пользователей к ресурсам ЗС ОДПГ осуществляет ответственное лицо органа государственной власти или органа местного самоуправления (далее – ответственное лицо).

## **2.2. Перечень мероприятий по подключению АРМ пользователей**

Подключение АРМ пользователей к ЗС ОДПГ производится путем выполнения следующих мероприятий:

- Регистрация пользователей.
- Получение установочных комплектов.
- Получение дистрибутивов ключей.
- Подключение АРМ пользователей.

### **2.2.1. Регистрация пользователей**

В государственных органах и органах местного самоуправления, где планируется подключение АРМ пользователей к ресурсам ЗС ОДПГ, ответственным лицом выполняется регистрация пользователей АРМ.

Регистрация пользователей производится на сайте ССТУ.РФ с использованием выданного логина и пароля при проведении общероссийского дня приема граждан в 2013 году.

### **2.2.2. Получение установочных комплектов**

Для получения установочных комплектов ответственное лицо обращается либо к производителю средств защиты ОАО «ИнфоТеКС», либо к его официальному партнёру с заявкой на приобретение необходимого количества комплектов ПО ViPNet Client (класс криптозащиты КС1 по требованиям ФСБ России). Постоянно обновляемый перечень официальных партнёров ОАО «ИнфоТеКС» приведён на сайте <http://www.infotecs.ru/partners/list/>. Форма заявки приведена в приложении 1.

Заявка отправляется по электронной почте в адрес ОАО «ИнфоТеКС» [soft@infotecs.ru](mailto:soft@infotecs.ru), факс +7 (495) 737-72-78 или в адрес официального партнёра ОАО «ИнфоТеКС».

Результатом обращения является приобретение ответственным лицом необходимого количества комплектов ПО ViPNet Client для установки на АРМ пользователей.



### **2.2.3. Передача дистрибутива ключей**

После получения необходимого количества комплектов ПО ViPNet Client ответственное лицо обращается в региональный центр Спецсвязи ФСО России за получением дистрибутива ключей. Уполномоченное лицо регионального центра спецсвязи ФСО России (далее – уполномоченное лицо) передает ответственному лицу необходимое количество дистрибутивов ключей (файлы с расширением DST).

### **2.2.4. Подключение АРМ пользователя**

Перед подключением АРМ пользователя ответственное лицо регистрирует полученные комплекты ПО ViPNet Client и дистрибутивов ключей в журнале поэкземплярного учета СКЗИ (приложение 3).

Решение о том, кто выполняет установку и настройку ПО ViPNet Client на АРМ пользователей, принимается ответственным лицом государственного органа или органа местного самоуправления, в ведении которых находятся АРМ пользователей (силами пользователей данных АРМ, специалистами IT-подразделения или с привлечением специалистов официальных партнеров ОАО «ИнфоТеКС»).

Для подключения АРМ пользователей к ресурсам ЗС ОДПГ производится установка и настройка ПО ViPNet Client на АРМ пользователей с использованием дистрибутивов ключей (файлов с расширением DST).

Хранение носителей с дистрибутивами ключей, установочных комплектов ПО ViPNet Client, комплектов эксплуатационной и технической документации, полученные для установки и настройки ПО ViPNet Client, осуществляется в специальном хранилище. Учет хранилища фиксируется в журнале учета хранилищ (приложение 4).

### **2.3. Эксплуатация АРМ пользователей**

За эксплуатацию и обслуживание АРМ пользователей, а также установленного на них ПО отвечает ответственное лицо государственного органа или органа местного самоуправления, в ведении которого находятся АРМ пользователей.

В случае выхода АРМ пользователя из строя (отказ программного или аппаратного обеспечения) настройка его аппаратного или программного обеспечения производится силами специалистов государственного органа или органа местного самоуправления.

### **2.4. Техническое сопровождение ПО ViPNet Client**

Сопровождение и консультации ответственных лиц по вопросам, связанным с эксплуатацией ПО ViPNet Client, при наличии сертификата технической поддержки, обеспечивают специалисты ОАО «ИнфоТеКС».

Специалисты ОАО «ИнфоТеКС» предоставляют следующие услуги по техническому сопровождению:

Обновление ПО ViPNet Client при выходе новых версий, прошедших сертификацию.

Консультации по ПО ViPNet Client и ответы на вопросы по электронной почте: [hotline@infotecs.ru](mailto:hotline@infotecs.ru) и по «горячей» телефонной линии: +7 (495) 737-6196.

Услуги предоставляются во временный период с 9:00 до 18:00 часов московского времени по рабочим дням.

### **3. Технические требования к подключению АРМ пользователей к ЗС ОДПГ**

#### **3.1. Требования к организации подключения к ЗС ОДПГ**

- 3.1.1. Для подключения АРМ пользователя к ЗС ОДПГ необходимо включить его в состав региональной VPN-сети.
- 3.1.2. Для обеспечения защищенного взаимодействия АРМ пользователя с региональной VPN-сетью на него должно быть установлено средство защиты, выполняющее функции криптографической защиты данных и межсетевое экранирование.
- 3.1.3. В качестве средства защиты информации необходимо использовать ПК ViPNet Client, сертифицированный ФСБ России как шифровальное (криптографическое) средство защиты по классу КС1 и как межсетевой экран по 4 классу защищенности.
- 3.1.4. Возможность подключения АРМ пользователей, оборудованных сертифицированными ФСБ России средствами защиты ViPNet, к ЗС ОДПГ обеспечивается переводом (путем переподчинения) таких АРМ пользователей в состав ЗС ОДПГ.
- 3.1.5. Решение о возможности подключения АРМ пользователей, входящих в состав сторонних VPN-сетей, реализованных с помощью сертифицированных ФСБ России средств защиты ViPNet, к ЗС ОДПГ путем организации меж сетевого взаимодействия принимается индивидуально в каждом конкретном случае по согласованию со Спецсвязью ФСО России, а также с учетом доработки и согласования с регуляторами в области информационной безопасности (далее – ИБ) моделей угроз и нарушителя ИБ данных сетей.
- 3.1.6. Допускается использование в качестве средства защиты информации АРМа пользователя ПАК ViPNet HW-1000, установленные в высших региональных государственных органах исполнительной власти в составе ССТУ, с соответствующей адресацией. В этом случае следует

учитывать, что адресное пространство для АРМ пользователей в сети ССТУ ограничено адресом 10.1.хх.71-10.1.хх.127 (где хх изменяется в зависимости от региона, в котором расположен НВ-1000 ССТУ РОИВ).

- 3.1.7. Допускается использование в качестве средства защиты информации АРМ пользователя ПАК ViPNet НВ-1000, установленные в высших региональных государственных органах исполнительной власти в составе ССТУ, с соответствующей адресацией. В этом случае следует учитывать, что адресное пространство для АРМ пользователей в сети ССТУ ограничено диапазоном адресов 10.1.хх.71-10.1.хх.127 (где хх изменяется в зависимости от региона, в котором расположен НВ-1000 ССТУ РОИВ).
- 3.1.8. В случае использование в качестве средства защиты информации АРМ пользователя ПАК ViPNet НВ-1000, недопускается подключение АРМ пользователей к сети международного информационного обмена Интернет.
- 3.1.9. Типовая схема подключения АРМ пользователя к ЗС ОДПГ представлена на рисунке 1.

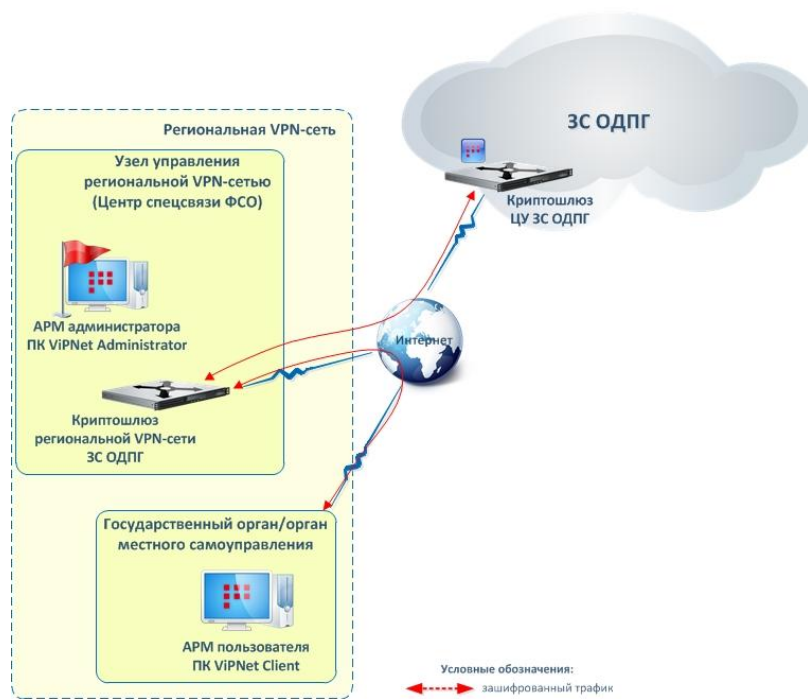


Рисунок 2. Типовая схема подключения АРМ пользователя к ЗС ОДПГ

## 3.2. Требования к АРМ пользователя

3.2.1. Требования к составу технических средств и операционным системам АРМ пользователя:

- процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;
- объем оперативной памяти — не менее 512 Мбайт (рекомендуется 1 Гбайт);
- свободное место на жестком диске — не менее 250 Мбайт (рекомендуется 500 Мбайт);
- сетевой адаптер или модем;
- операционная система (далее – ОС) — Windows XP SP3 (32-разрядная)/Vista SP2 (32/64-разрядная)/Windows 7 (32/64-разрядная).

3.2.2. На АРМ пользователя должна быть установлена одна ОС.

3.2.3. Установку должен выполнять пользователь, обладающий правами администратора в ОС Windows.

3.2.4. На АРМ пользователя должны быть установлены программные средства защиты информации от компьютерных вирусов и вредоносных воздействий.

3.2.5. В BIOS должен быть установлен один вариант загрузки ОС – с жесткого диска, все альтернативные варианты загрузки должны быть отключены, в том числе сетевая загрузка.

3.2.6. На АРМ пользователя должны быть выполнены корректные настройки часового пояса, даты и времени.

3.2.7. Если на АРМ пользователя установлена ОС Windows, локализация которой отличается от русской, то для правильного отображения

кириллицы в интерфейсе ПК ViPNet Client необходимо установить поддержку кириллицы для программ, не поддерживающих Unicode.

- 3.2.8. Запрещаться пользоваться отладочными версиями ОС, такими как Debug/Checked Build, а также устанавливать средства отладки и трассировки программного обеспечения.
- 3.2.9. На АРМ пользователя должны быть отключены сторонние межсетевые экраны и приложения, обеспечивающие преобразование сетевых адресов (NAT).
- 3.2.10. При наличии на АРМ пользователя ранее установленного ПК ViPNet Client, выполнявшего функции подключения к ЗС ОДПГ в 2013 г., необходимо произвести деинсталляцию данного ПК.

### **3.3. Требования к каналам связи**

- 3.3.1. Для передачи данных в ЗС ОДПГ АРМ пользователя должен быть подключен к каналам сети связи общего пользования.
- 3.3.2. Пропускная способность канала связи должна быть не менее 1024 Кбит/с.
- 3.3.3. При наличии внешнего межсетевого экрана необходимо обеспечить прохождение пакетов протокола UDP с портом источника 55777 из внутренней (локальной сети) во внешнюю (Интернет) с подменой IP-адреса локальной сети на IP-адрес сети Интернет без смены портов и ответный трафик (NAT).

### **3.4. Организационные требования**

- 3.4.1. Необходимо назначить ответственное лицо органа государственной власти либо органа местного самоуправления для организации подключения АРМ пользователя к региональной VPN-сети ЗС ОДПГ.
- 3.4.2. Для хранения носителей с ключевой информацией, установочный комплект, эксплуатационной и технической документации,

полученные для установки и настройки ПК ViPNet Client, должно быть предусмотрено надежное металлическое хранилище, оборудованное внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин.

- 3.4.3. Необходимо наличие журнала учета хранилищ (образец журнала в Приложении 1), в котором будут содержаться носители, перечисленные в п. 2.4.2 и журнала поэкземплярного учета используемых средств криптографической защиты информации (образец журнала в Приложении 2).
- 3.4.4. После подключения АРМ пользователя к региональной VPN-сети, ответственным лицом должен быть составлен Акт подключения АРМ пользователя к ЗС ОДПГ в 2-х экземплярах с обязательной отметкой о соответствии требованиям настоящих ТУ. Один экземпляр остается в государственной структуре, эксплуатирующей АРМ пользователя, второй экземпляр передается в подразделение, эксплуатирующее узел управления региональной VPN-сети.
- 3.4.5. Помещения, в которых расположены АРМ пользователей, должны быть оборудованы средствами вентиляции и кондиционирования воздуха, которые должны соответствовать санитарно-гигиеническим нормам СНиП, устанавливаемым законодательством Российской Федерации.





**Приложение 2. Образец журнала поэкземплярного учета используемых средств криптографической защиты информации (СКЗИ)**

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или ФИО сотрудника органа криптографической защиты, изготовившего ключевые документы	Дата и номер сопроводительного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводительного письма	Дата и номер подтверждения или расписка в получении
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>	<b>16</b>

## Форма заявки на приобретение ПО ViPNet Клиент (КС1)<sup>1</sup>

1	Название организации покупателя в соответствии с учредительными документами	
2	ИНН организации	
3	КПП организации	
4	Юридический адрес	
5	Фактический адрес	
6	Телефон/факс с кодом города	
7	Расчетный счет	
8	БИК банка организации	
9	Необходимое количество лицензий на ПО ViPNet Клиент (КС1)	
10	Номер или название защищенной ViPNet-сети, к которой будет осуществляться подключение	См. стр.22 Приложение 6.
12	ФИО контактного лица	
13	E-mail контактного лица/организации	
14	ФИО лица подписывающего договор со стороны покупателя.	
15	Основание дающие право подписания. (№ и дата доверенности, устав или положение)	

<sup>1</sup> Если организация - конечный пользователь ПО ViPNet Клиент (КС1) является филиалом или обособленным подразделением, то необходимо указать реквизиты и главной организации и филиала, а именно пункты 1,2,3,4,7,8 приведенной выше таблицы заполняются дважды. Первый раз с указанием реквизитов конечного пользователя филиала и второй раз с указанием реквизитов головной организации.

**Образец журнала поэкземплярного учета используемых средств  
криптографической защиты информации (СКЗИ)**

№ п/п	Наименование СКЗИ, эксплуатационной и технической документации к ним, ключевых документов	Серийные номера СКЗИ, эксплуатацион- ной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографи- ческие номера) ключевых документов	Отметка о получении		Отметка о рассылке (передаче)		
				От кого получены или ФИО сотрудника органа криптографическ ой защиты, изготовившего ключевые документы	Дата и номер сопроводитель- ного письма или дата изготовления ключевых документов и расписка в изготовлении	Кому разосланы (переданы)	Дата и номер сопроводитель- ного письма	Дата и номер подтверждения или расписка в получении
<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>	<b>6</b>	<b>7</b>	<b>8</b>	<b>9</b>

Отметка о возврате		Дата ввода в действие	Дата вывода из действия	Отметка об уничтожении СКЗИ, ключевых документов		Примечание
Дата и номер сопроводительного письма	Дата и номер подтверждения			Дата уничтожения	Номер акта или расписка об уничтожении	
<b>10</b>	<b>11</b>	<b>12</b>	<b>13</b>	<b>14</b>	<b>15</b>	<b>16</b>



## Приложение-6: Номера сетей ViPNet

Номер сети (нумерация ИнфоТеКС)	Название региона
3325	Адыгея республика
3326	Алтай республика
3327	Алтайский край республика
3328	Амурская область
3329	Архангельская область
3330	Астраханская область
3331	Ненецкий автономный округ
3332	Башкортостан республика
3334	Белгородская область
3343	Брянская область
3344	Бурятия республика
3345	Владимирская область
3346	Волгоградская область
3347	Вологодская область
3348	Воронежская область
3349	Дагестан республика
3350	Еврейский автономный округ
3351	Забайкальский край
3352	Ивановская область
3353	Ингушетия республика
3354	Иркутская область
3355	Кабардино-Балкарская республика
3356	Калининградская область

3357	Калмыкия республика
3358	Калужская область
3359	Камчатский край
3360	Карачаево-Черкессия республика
3361	Карелия республика
3362	Кемеровская область
3363	Кировская область
3364	Коми республика
3365	Костромская область
3366	Краснодарский край
3367	Красноярский край
3368	Курганская область
3369	Курская область
3370	Ленинградская область
3371	Липецкая область
3372	Магаданская область
3373	Марий-Эл республика
3374	Мордовия республика
3375	Москва город
3376	Московская область
3377	Мурманская область
3378	Нижегородская область
3379	Новгородская область
3380	Новосибирская область
3381	Омская область
3382	Оренбургская область
3383	Орловская область
3384	Пензенская область

3385	Пермский край
3386	Приморский край
3387	Псковская область
3388	Ростовская область
3389	Рязанская область
3390	Самарская область
3391	Санкт-Петербург город
3392	Саратовская область
3393	Саха (Якутия) республика
3394	Сахалинская область
3395	Свердловская область
3396	Северная Осетия-Алания республика
3397	Смоленская область
3398	Ставропольский край
3399	Тамбовская область
3400	Татарстан республика
3401	Тверская область
3402	Томская область
3403	Тульская область
3404	Тыва республика
3405	Тюменская область
3406	Удмуртская республика
3407	Ульяновская область
3408	Хабаровский край
3409	Хакасия республика
3410	Ханты-Мансийский автономный округ
3411	Челябинская область
3412	Чеченская республика



3413	<b>Чувашия республика</b>
3414	<b>Чукотский автономный округ</b>
3415	<b>Ямало-Ненецкий автономный округ</b>
3416	<b>Ярославская область</b>
3597	<b>Федеральные органы исполнительной власти и их территориальные подразделения</b>