ПРИЛОЖЕНИЕ 1

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

на создание виртуальной защищенной частной сети **(VPN)**

Настоящие Технические требования разработаны в соответствии с Техническим заданием (ТЗ) на создание корпоративной информационной сети.

В документе описываются технические требования на создание виртуальной защищенной частной сети информационно-коммуникационной системы ЦАРИКЦ.

1. Общие требования

1.1. Виртуальная защищенная частная сеть (Virtual Private Network - VPN) должна иметь централизованное управление всей сетью и политикой безопасности функционирования защищенных узлов, а также созданной ключевой структуры, с возможностью локальной настройки отдельных узлов.

1.2. VPN должна создаваться с использованием программных и/или программно-аппаратных средств - межсетевых экранов с криптошлюзом, персональных сетевых экранов с криптошлюзом, а также программных средств криптосервиса.

1.3. VPN. должна иметь единую криптографическую подсистему, которая, в свою очередь, должна обеспечивать шифрование и подписание электронной цифровой подписью (ЭЦП), а также шифрование произвольного IP-трафика между узлами VPN (межсетевыми экранами, между рабочими местами пользователей и межсетевыми экранами, между всеми рабочими местами пользователей).

1.4. В криптографической подсистеме VPN должны быть использованы криптографические алгоритмы по следующим стандартам:

- Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;
- Информационная технология. Криптографическая защита информации. Функция хэширования;
- Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных;

1.5. В VPN могут быть использованы средства криптографической защиты информации (СКЗИ) зарубежного производства в том случае, если в них реализованы криптографические алгоритмы по стандартам, перечисленные в п.1.4 настоящего документа, с предварительным согласованием их использования в Уполномоченном органе в области криптографической защиты информации.

2. Требования к структуре VPN

2.1. Структура VPN должна соответствовать инфраструктуре и должна рассматриваться как множество узлов, связанных между собой виртуальными каналами передачи данных.

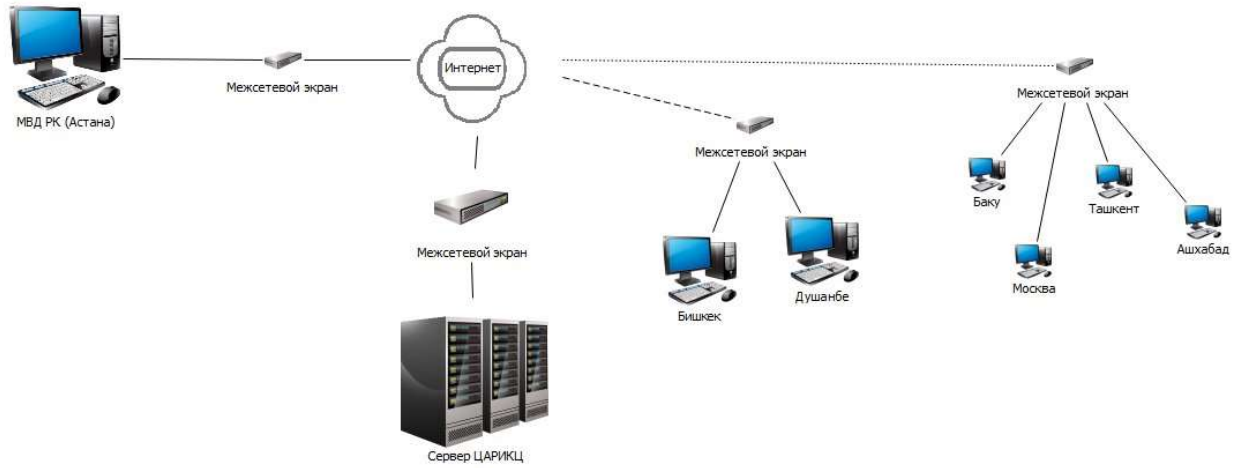
2.2. В соответствии с описанными ветвями в VPN должны быть предусмотрены узлы следующего уровня (рис.):

- центральный узел в г.Алматы (Первый этап);
- узел, расположенный в г.Астана, в МВД Республики Казахстан (Первый этап);
- узлы, расположенные в г.г.Бишкек и Душанбе (Второй этап);
- узлы, расположенные в г.г.Баку, Ташкент, Ашхабад и Москва (Третий этап).

Всего 7 узлов, с возможностью расширения до 20-30 узлов.

2.3. Центральный узел VPN должен представлять собой программно-аппаратный комплекс управления VPN в целом и её узлами, т.е. выполнять функции центра управления сетью (ЦУС VPN). ЦУС VPN должен располагаться в г. Алматы, в здании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров **(ЦАРИКЦ)**.

2.4. Узлы подключения представляют собой локальную вычислительную сеть (ЛВС), которые будут подключаться к ЦУС через межсетевые экраны с криптошлюзом, устанавливаемые на серверах ЛВС компетентных органов государств-участников ЦАРИКЦ.



3. Программно-аппаратные средства

3.1. Программно-аппаратные средства на каждый узел соединения будут предоставлены заказчиком.

3.2. Примерный перечень используемых программно-аппаратных средств:

Cisco Firepower	
Firepower Threat Defense	
Cisco Firepower Management Center for 25 devices	