

Типовая схема построения географически распределенной сети ведомства с использованием симметричной и несимметричной ключевых схем (комбинированное решение)

Комбинированное решение использует симметричную и несимметричную ключевые схемы распределения ключей. Симметричная ключевая схема позволяет достигать сравнительно больших скоростей шифрования (приблизительно на 30 % больше по сравнению с несимметричной ключевой схемой распределения) и не требует разворачивания сложной инфраструктуры, поэтому для защиты магистральных каналов связи в крупной географически распределенной сети организации целесообразно использовать VPN-туннели с применением симметричной ключевой схемы распределения. Для построения подчиненных защищенных сетей целесообразно использовать несимметричную ключевую схему из-за разветвленности и постоянного роста этих сетей, а также из-за большого количества удаленных мобильных абонентов. При использовании несимметричной ключевой схемы возможно интегрировать программные и аппаратные решения компании «Фактор-ТС» в уже существующую инфраструктуру PKI с использованием существующих у заказчика удостоверяющих центров. Криptomаршрутизаторы крупных региональных центров находятся на границе двух ключевых схем и осуществляют перешифрование и перенаправление трафика из одного типа VPN-туннелей в другой. На рис. 6 изображена типовая схема реализации комбинирования ключевых схем.

Необходимое оборудование и ПО	Назначение	Производитель
Несимметричная ключевая схема		
Криptomаршрутизатор ПАК Dionis DPS	Сервер доступа для абонентов	«Фактор-ТС»
Криptomаршрутизатор ПАК Dionis DPS	Клиент сервера доступа и МЭ для ЛВС	«Фактор-ТС»
Программное обеспечение DiSec	Подключение к серверу доступа	«Фактор-ТС»
Удостоверяющий центр (УЦ)	Управление инфраструктурой PKI	«Крипто-ПРО»
ПО МГК (модуль генерации ключей)	Выпуск сертификатов по запросу	«Фактор-ТС»
ПО оператора УЦ	Генерация запросов на сертификат	«Крипто-ПРО»
Электронный токен («Рутокен»)	Хранение ключей и сертификатов	«Актив»
Планшет, ноутбук (Windows)	Установка ПО DiSec	Lenovo, Asus
Межсетевой экран (ФСБ МЭЗ)	Защита УЦ от внешних угроз	Любой
АПМДЗ (ФСБ) (для рабочих мест)	Для класса защищенности КС2, КС3	Setec, «Анкад»
Симметричная ключевая схема		
Криptomаршрутизатор Dionis DPS	Шифрование потока данных	«Фактор-ТС»
Центр управления сетью	Мониторинг и управление	«Фактор-ТС»
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»
USB-флеш-диск	Хранение ключей шифрования	Любой

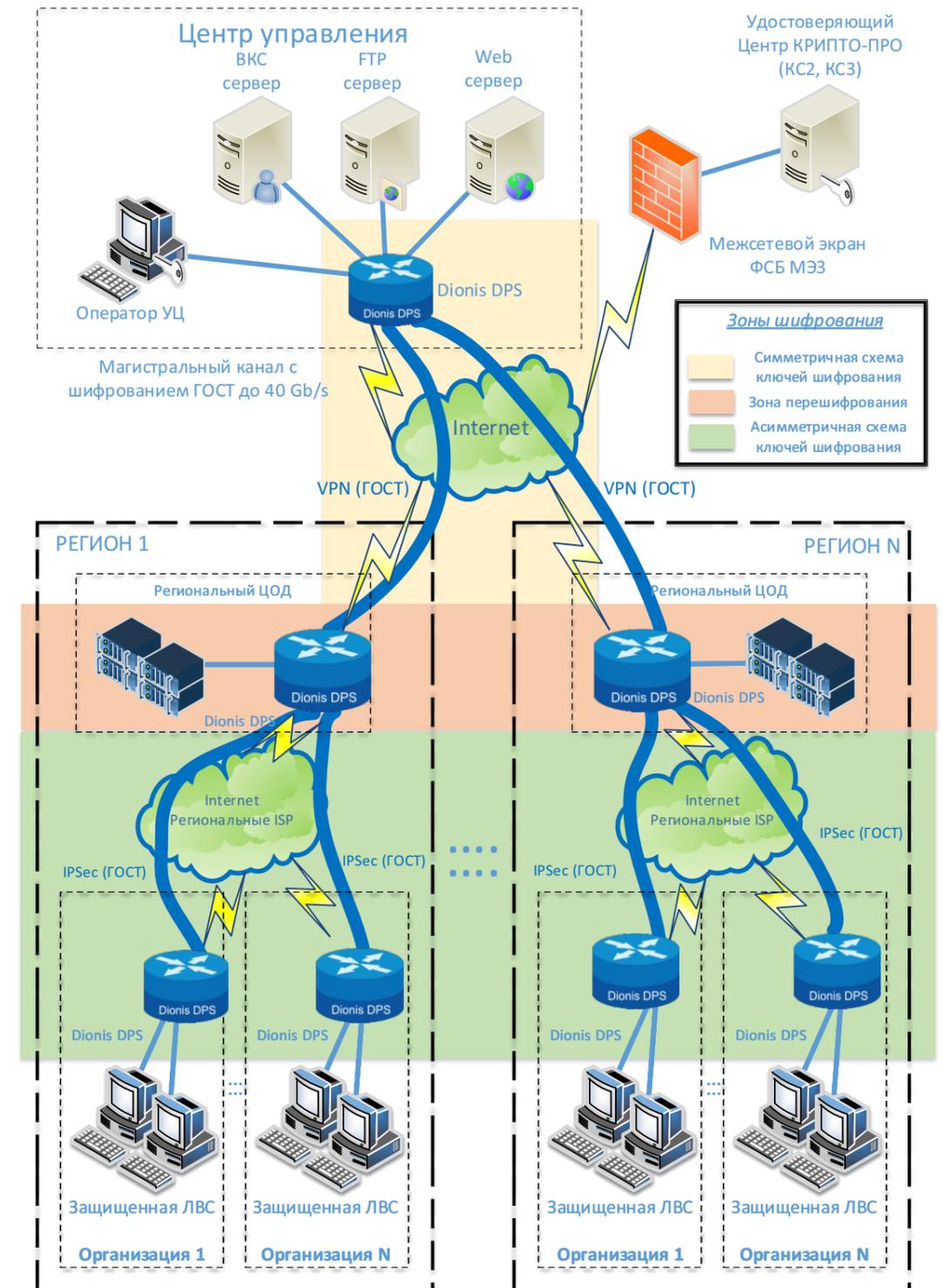


Рис. 6. Типовая схема построения географически распределенной сети ведомства с использованием симметричной и несимметричной ключевых схем