

Построение защищенной корпоративной сети на базе несимметричной ключевой схемы (PKI) с использованием протокола IPSec (ГОСТ). Класс защиты КС1, КС3

Решение имеет клиент-серверную архитектуру, такую же, как и в случае с организацией удаленного защищенного доступа мобильных абонентов (стр. 10), но при такой реализации в качестве клиентов центрального сервера доступа могут выступать сами ПАК Dionis DPS, за которыми находятся защищаемые ЛВС. ПАК Dionis DPS и клиентское ПО DiSec поддерживают технологию NAT Traversal, что позволяет всем подчиненным подразделениям и удаленным пользователям, кроме центрального узла, использовать динамические IP-адреса, получаемые по протоколу DHCP от провайдера. Услуги по предоставлению клиентам открытых и закрытых ключей выполняет удостоверяющий центр (УЦ) «Крипто-ПРО» или иной УЦ. Для генерации закрытых ключей и запросов к УЦ на выдачу сертификатов на стороне удаленных пользователей используется программное обеспечение «МГК-3» производства ООО «Фактор-ТС». Для хранения ключевой информации используется криптографический USB-токен (Rutoken, eToken), съемный USB-носитель и т. п. Реализуемый класс защиты КС2, КС3 (для класса КС3 на рабочих станциях необходимо дополнительно использовать сертифицированные ФСБ средства защиты, например АПМДЗ). На рис. 2 изображена типовая схема реализации.

| Необходимое оборудование и ПО | Назначение | Производитель |
|--|-------------------------------------|----------------|
| Криптомаршрутизатор ПАК Dionis DPS | Сервер доступа для абонентов | «Фактор-ТС» |
| Криптомаршрутизатор ПАК Dionis DPS | Клиент сервера доступа и МЭ для ЛВС | «Фактор-ТС» |
| Программное обеспечение DiSec (клиент) | Подключение к серверу доступа | «Фактор-ТС» |
| Удостоверяющий центр (УЦ) | Управление инфраструктурой PKI | «Крипто-ПРО» |
| ПО МГК-4 (модуль генерации ключей) | Генерация запросов на сертификат | «Фактор-ТС» |
| ПО оператора УЦ | Выпуск сертификатов по запросу | «Крипто-ПРО» |
| Электронный токен («Рутокен») | Хранение ключей и сертификатов | «Актив» |
| Планшет, ноутбук (OS Windows) | Установка ПО DiSec | Lenovo, Asus |
| Межсетевой экран (ФСБ МЭЗ) | Защита УЦ от внешних угроз | Любой |
| АПМДЗ (ФСБ) (для рабочих станций) | Для класса защищенности КС2, КС3 | Setec, «Анкад» |

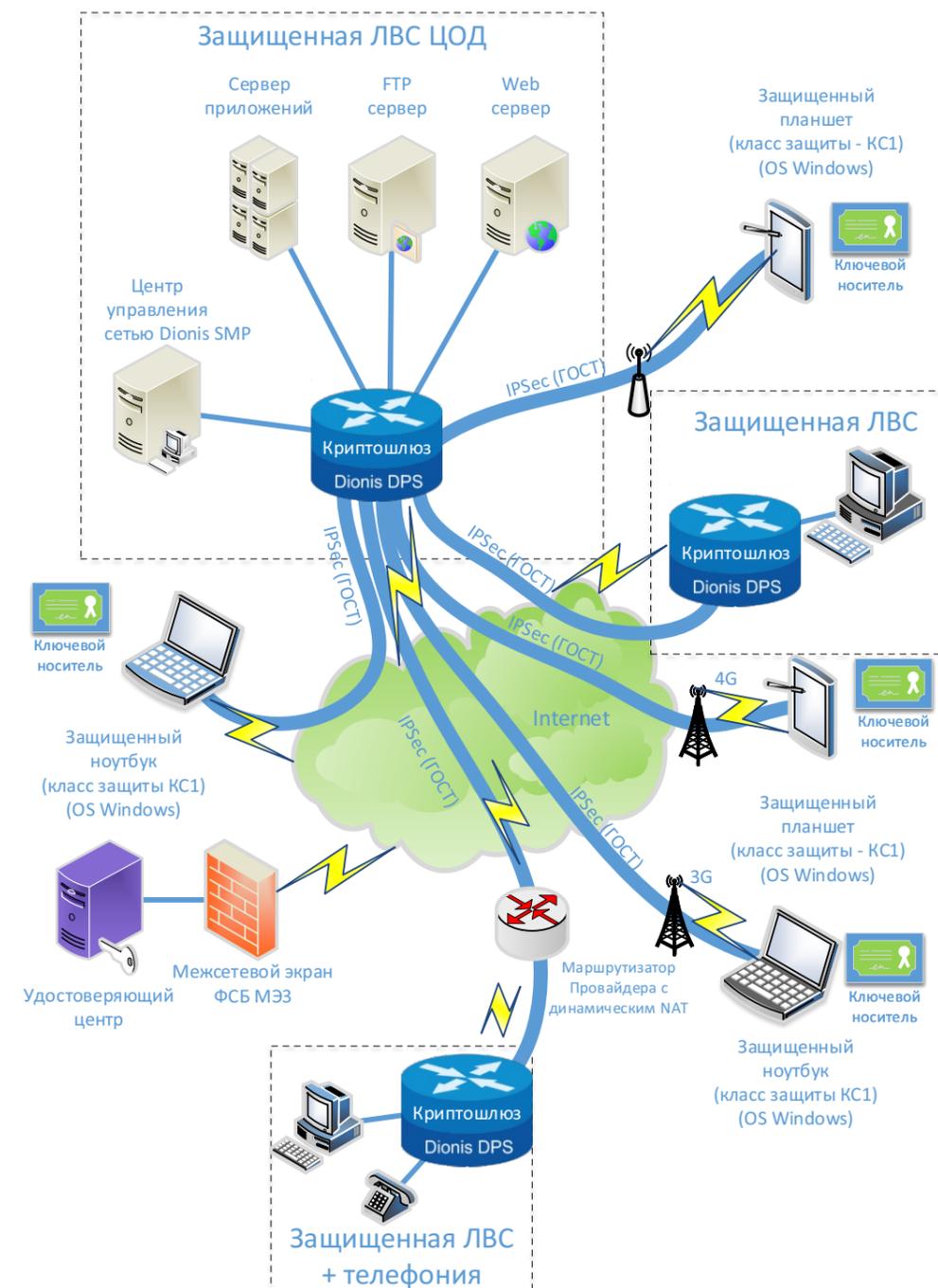


Рис. 2. Построение защищенной корпоративной сети на базе несимметричной ключевой схемы (PKI) с использованием протокола IPSec (ГОСТ). Класс защиты КС1, КС3