

## Построение защищенной ведомственной сети с использованием симметричной ключевой схемы

Данное решение может быть построено по схеме «звезда» (такой вариант является частным примером, так как защищенная сеть может быть развернута и по принципу «каждый с каждым» или иным способом). Локальная вычислительная сеть (ЛВС) подчиненного удаленного подразделения защищена межсетевым экраном ПАК Dionis DPS, который также является и криптомаршрутизатором. Каждый криптомаршрутизатор ПАК Dionis DPS удаленного подразделения связан одним криптографическим VPN-туннелем (ГОСТ 28147-89) для защищенного обмена данными с центральным узлом, а также отдельным криптографическим туннелем (можно не использовать выделенный туннель для управления), через который проходит поток управления подчиненным узлом из центра управления сетью. Вся связь между подчиненными криптомаршрутизаторами и защищаемыми ими ЛВС происходит через криптомаршрутизатор центрального узла. Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства ООО «Фактор-ТС». Ключи записываются на USB-флеш-диски и доверенным способом доставляются на каждый узел. Возможно сгенерировать несколько ключей шифрования для каждого узла, чтобы одновременно загрузить их на узел и обеспечить автономность работы без необходимости физического доступа к узлу при плановой смене ключей шифрования. Плановую смену ключей можно выполнять при помощи центра управления сетью (Dionis SMP) по защищенному туннелю управления. По защищенному туннелю сами ключи шифрования не пересылаются; из Dionis SMP подается команда о замене старого ключа на новый, заранее загруженный при первом вводе ключей. На рис. 4 изображена типовая схема построения корпоративной сети с использованием симметричной ключевой схемы.

| Необходимое оборудование и ПО      | Назначение                  | Производитель |
|------------------------------------|-----------------------------|---------------|
| Криптомаршрутизатор ПАК 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         |

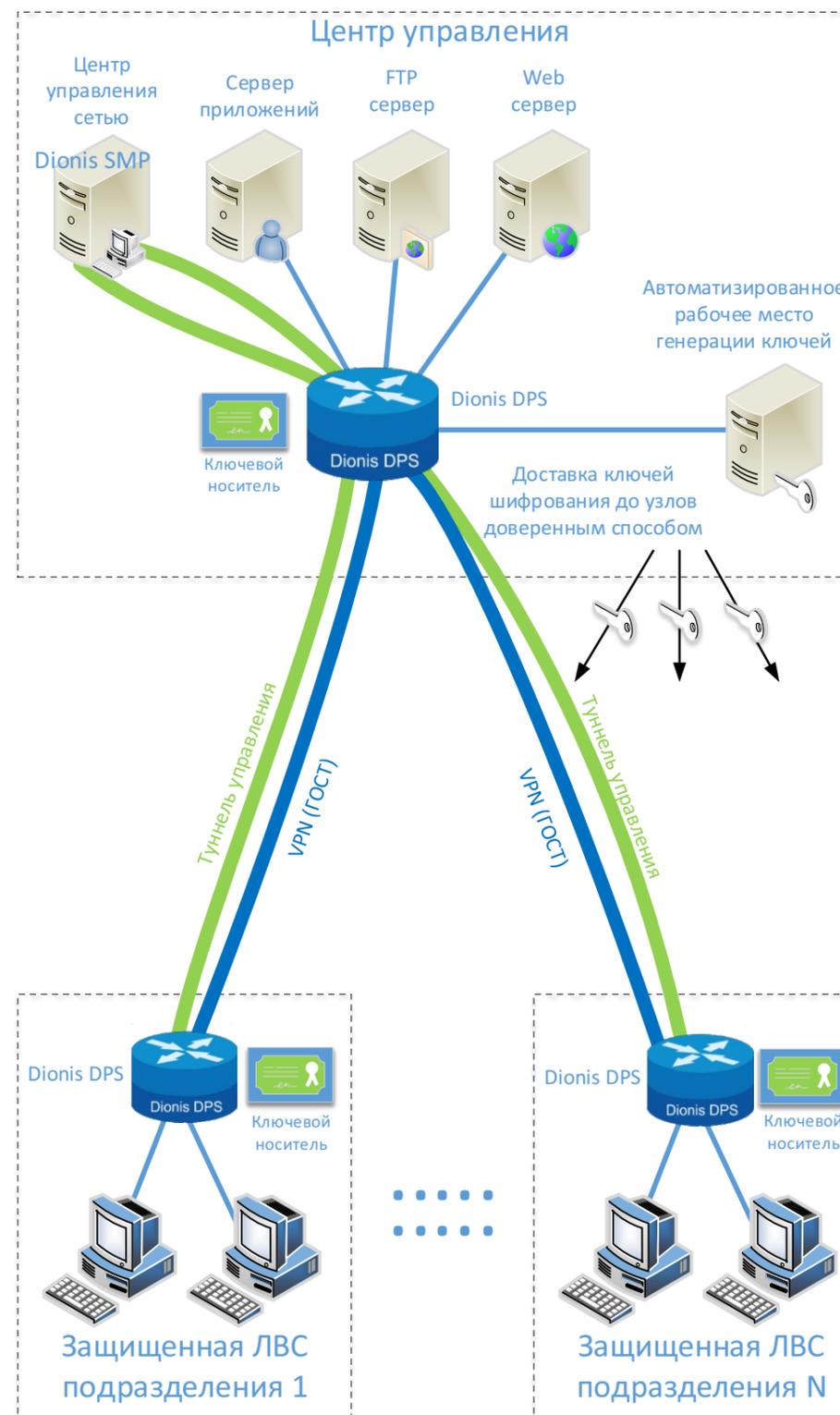


Рис. 4. Построение защищенной ведомственной сети с использованием симметричной ключевой схемы