

Криптомаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147-89) со скоростью шифрования до 10 Гб/с

Данное решение позволяет организовать защищенный поток передачи данных (шифрование ГОСТ 28147-89) на скорости до 10 Гб/с при наличии нескольких каналов от разных провайдеров, не связанных между собой автономной системой. Для примера на рис. 5.1 приведена схема взаимодействия между основным центром обработки данных (ЦОД 1) и удаленным (ЦОД 2).

Изделия ПАК Dionis DPS используются в данной схеме не только как криптомаршрутизаторы (Dionis DPS 3 и Dionis DPS 4), но и как балансировщики нагрузки (Dionis DPS 1 и Dionis DPS 2). Задача балансировщика нагрузки — равномерно распределить трафик, поступающий из внутренней сети ЦОД, между криптомаршрутизаторами Dionis DPS 3 и Dionis DPS 4. Балансировщики Dionis DPS 1 и Dionis DPS 2 объединены в отказоустойчивый кластер (HA, High-Availability) и дублируют друг друга. Криптомаршрутизаторы Dionis DPS 3 и Dionis DPS 4 работают одновременно со скоростями шифрования равным 6 Гб/с (UDP 1500) каждый, что в сумме дает скорость шифрования свыше 10 Гб/с. Устройства Dionis DPS 3 и Dionis DPS 4 соединены с внешним каналом передачи данных через пограничные маршрутизаторы, которые также дублируют друг друга. В случае выхода из строя одного из криптомаршрутизаторов схема останется работоспособной, но общая производительность шифрования снизится до 6 Гб/с. Схема на стороне удаленного ЦОД 2 идентична схеме на стороне ЦОД 1. Криптографические туннели на симметричных ключах шифрования создаются между Dionis DPS 3 и Dionis DPS 4 и между Dionis DPS 6 и Dionis DPS 5 соответственно. Симметричные ключи шифрования генерируются при помощи программы «Автоматизированное рабочее место генерации ключей» (АРМ ГК v.4) производства ООО «Фактор-ТС». Ключи записываются на USB носитель и доверенным способом доставляются на каждый узел. На рис. 5.1 изображена типовая схема реализации высокоскоростного и отказоустойчивого взаимодействия между ЦОД.

Необходимое оборудование и ПО	Назначение	Производитель
Маршрутизатор Dionis DPS	Балансировка нагрузки	«Фактор-ТС»
Криптомаршрутизатор Dionis DPS	Шифрование потока данных	«Фактор-ТС»
Коммутатор (SFP+)	Коммутация оптоволокну	Любой
Пограничный маршрутизатор	Обеспечение доступа к внешней сети	Любой
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»

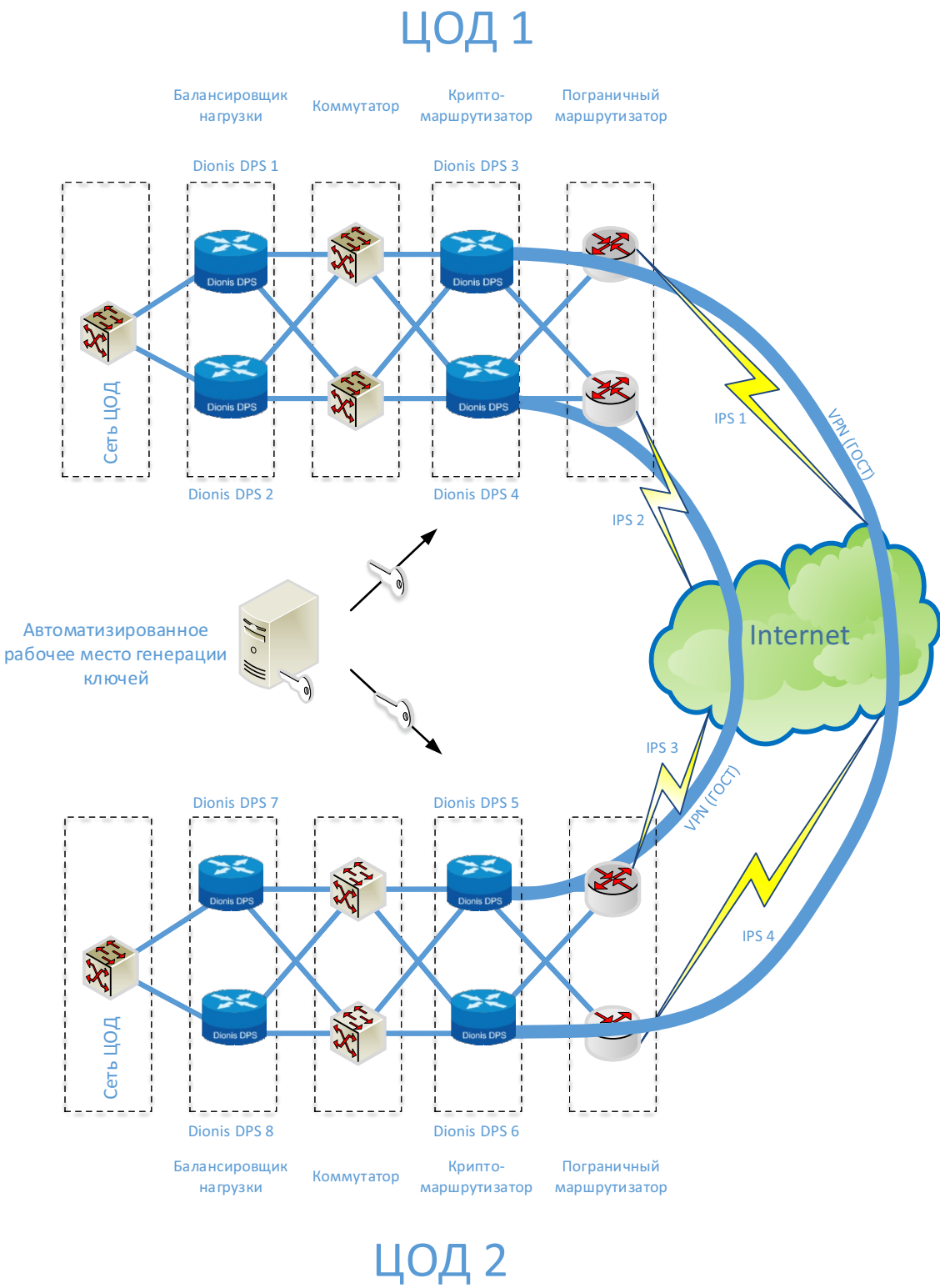


Рис. 5.1. Криптомаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147-89) со скоростью шифрования до 10 Гб/с при отсутствии автономной системы

Решение, изображенное на рис. 5.2, рекомендуется для использования при наличии автономной системы (AS) либо если есть планы по ее разворачиванию. Описанное решение позволяет организовать защищенный поток передачи данных с шифрованием по ГОСТ 28147-89 на скорости до 10 Гб/с.

Устройства Dionis DPS используются в данной схеме для решения двух задач: в качестве пограничных маршрутизаторов, принимающих анонсы BGP FullView от провайдеров, и в качестве криптошлюзов, объединенных в отказоустойчивый кластер (HA, High-Availability), для формирования зашифрованного соединения и обеспечения безопасности внутренних сетей ЦОД. Эти задачи специально разнесены по разным физическим устройствам для сохранения максимальной пропускной способности при пиковых нагрузках. При аварийном отключении одного из каналов связи стандартные механизмы работы протоколов BGP и OSPF приведут к автоматическому перераспределению трафика на рабочий канал, и таким образом препятствуют обрыву связи. То же самое произойдет и при выходе из строя одного из пограничных маршрутизаторов и/или коммутаторов. За счет использования отказоустойчивого кластера схема останется работоспособной даже при выходе из строя одного из криптошлюзов.

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, осуществляющий шифрование.

Назначение	Производитель	
Маршрутизаторы Dionis DPS	BGP-маршрутизация	«Фактор-ТС»
Криптошлюзы Dionis DPS	Шифрование потока данных и защита периметра внутренних сетей (МЭ)	«Фактор-ТС»
Коммутаторы (SFP+)	Коммутация оптоволоконных каналов связи	Любой управляемый коммутатор 2-го уровня
ПО АРМ ГК	Генерация ключей шифрования	«Фактор-ТС»

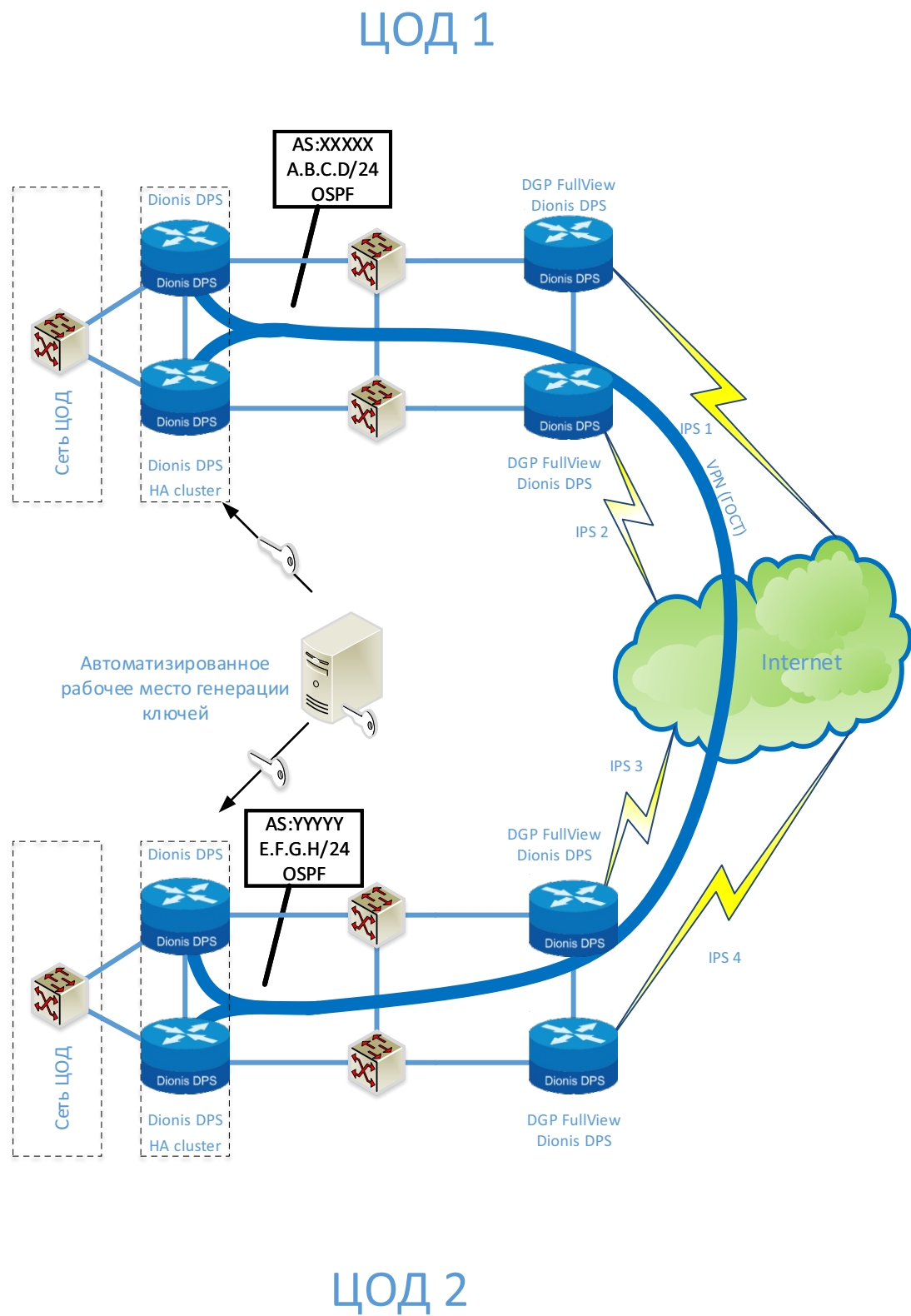


Рис. 5.2. Криptomаршрутизаторы для ЦОД. Создание защищенного канала связи (VPN ГОСТ 28147-89) со скоростью шифрования до 10 Гб/с при наличии автономной системы