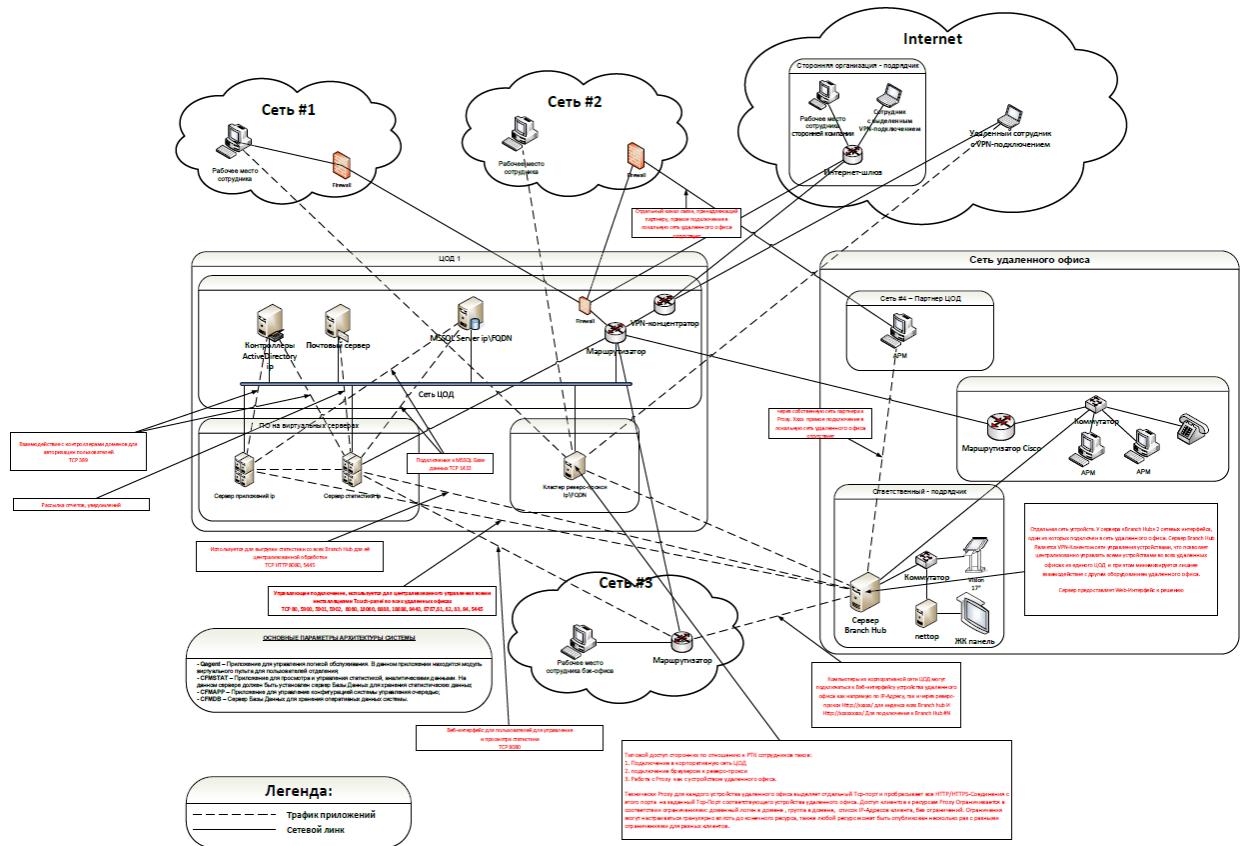


Хананиев Даниил Владимирович

Курс «Подготовка к собеседованию специалиста по информационной безопасности»,

поток от 20.05.2020

ДЗ № 3



1. Тут у нас 4 стороны. Клиент, ЦОД, Партнер ЦОД, сторонняя организация – подрядчик. Кроме клиента – владельца информации, доступ к какой-либо информации имеют сотрудники всех сторон. Т.е. необходимо согласовать минимальный уровень необходимой информации, требующейся для работы каждой стороны, и меры защиты этой информации. ЦОД с партнером и подрядчиком должны предоставить сертификаты соответствия нормам безопасности (по ISO) и документы последнего аудита.

2. Сеть организации в ЦОД-е, хоть физически и входит в сети ЦОД-а, но логически должна быть обособлена, т.е. должна иметь место отдельная виртуальная сеть VLAN.

3. HTTP(TCP/80, 8080) отказать. Только HTTPS.

4. Сеть #1 и Сеть #2 работают с ЦОД 1 через файрвол, ок, хотя VPN выглядит гораздо более безопасно и по best practices стандартно. Подрядчик и удаленный сотрудник через VPN, ок. Почему Сеть #3 и Сеть удаленного офиса напрямую, без vpn или файрвола подключаются к маршрутизатору? Непорядок.

Это все, в принципе, что я вижу на этом уровне.