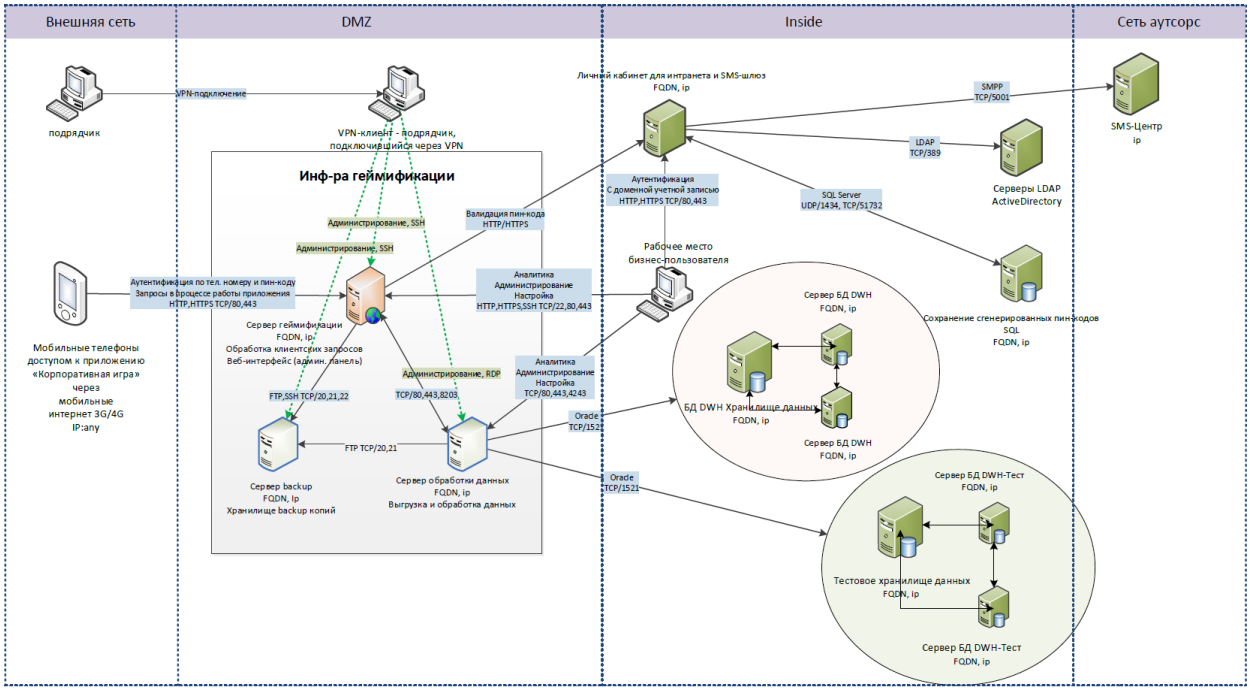
Хананиев Даниил Владимирович
Курс «Подготовка к собеседованию специалиста по информационной безопасности», поток от 20.05.2020
ДЗ № 5



1. Сразу отмечу, что надо использовать безопасные протоколы, я уже писал об этом во втором ДЗ, да и в общем, все замечания остаются в силе. В дальнейшем я не буду оглядываться на них

2. На входе DMZ, так и Inside сегментов, NIDS сенсоры, на серверах – HIDS и APIDS (если я правильно понимаю реализацию APIDS). Центральный сервер IPS в сегменте Inside, с защитой себя же.

3. Сервер SIEM в сегменте Inside, коннекторы ко всем серверам, работающим у них приложениям, БД, маршрутизаторам, хостам. Информация с IPS тоже должна сливаться в SIEM(тут у меня самого возникли вопросы о кооперации SIEM и IPS систем).

4. Сервера БД, защита от несанкционированного доступа. Физически - физическая охрана серверной, протоколы физического доступа строго определенных лиц, СКУД, журналируемая, логи опять же в SIEM, комплекс средств НСД для защиты физических сред передачи данных. И программно – запрет usb носителей и вообще полный контроль подключаемых носителей, строгий доступ пользователей согласно прав, следование принципу минимально необходимых привилегий. Все логи опять в SIEM. Принцип AAA, как всегда.

Как всегда, был бы бюджет, а куда его потратить всегда найдем. Надо смотреть на ценность защищаемых данных, свой бюджет, требования надзорных органов. Насколько нужен нам SIEM, это недешевое решение.