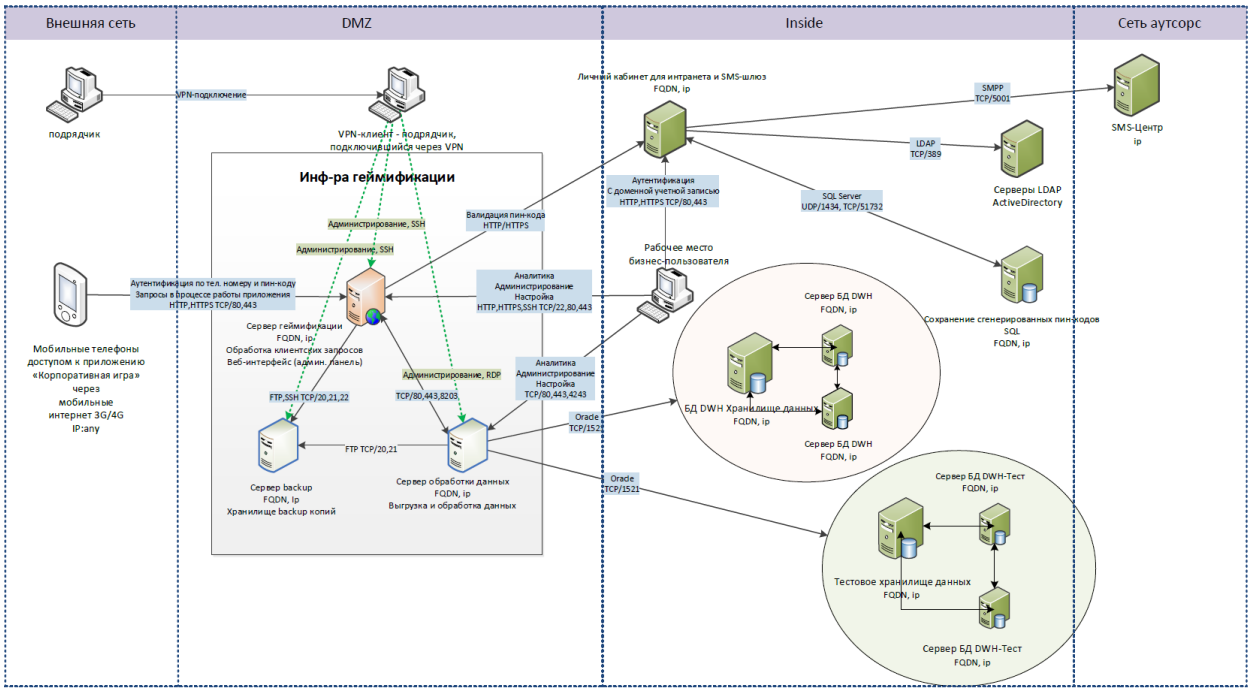
Хананиев Даниил Владимирович
Курс «Подготовка к собеседованию специалиста по информационной безопасности», поток от 20.05.2020
ДЗ № 2



1. Сразу скажу свое решительное «нет» незащищенным протоколам, таким как HTTP(TCP/80) и FTP(TCP/20,21).

2. Вся инфраструктура геймификации должна быть внутри периметра “Inside”, т.к. там содержатся данные пользователей (какие бы они не были), потому требуют защиты. Снаружи сервер авторизации и, м.б., сама логика игры. Данные, за которыми сервер будет обращаться, должны быть внутри, под защитой. Впрочем, сам игровой сервер я бы тоже внутрь поставил, сдается мне, что и основной игровой трафик будет идти с рабочих мест, тратить личное время для рабочей игры не думаю, что будет много желающих. В DMZ только сервер авторизации.

3. SSH и RDP только на ключах/сертификатах.

4. Излишне, наверно, но проговорю о файрволе, настроенному по белому списку и WAF со всем комплексом защиты на сервере в DMZ и рабочем сертификате для HTTPS.

5. best practice. Посмотрел я как примерно устроено в компаниях. Ничего подробного не нашел. Увидел много подрядчиков, предлагающих свои услуги в широком спектре, в том числе и на своих площадках. В этом случае, думаю, там не должны храниться данные пользователей. Каждый пользователь имеет свой логин/пароль, а сопоставление логинов и реальных пользователей и их достижений, соответственно, должно происходить уже внутри компании.