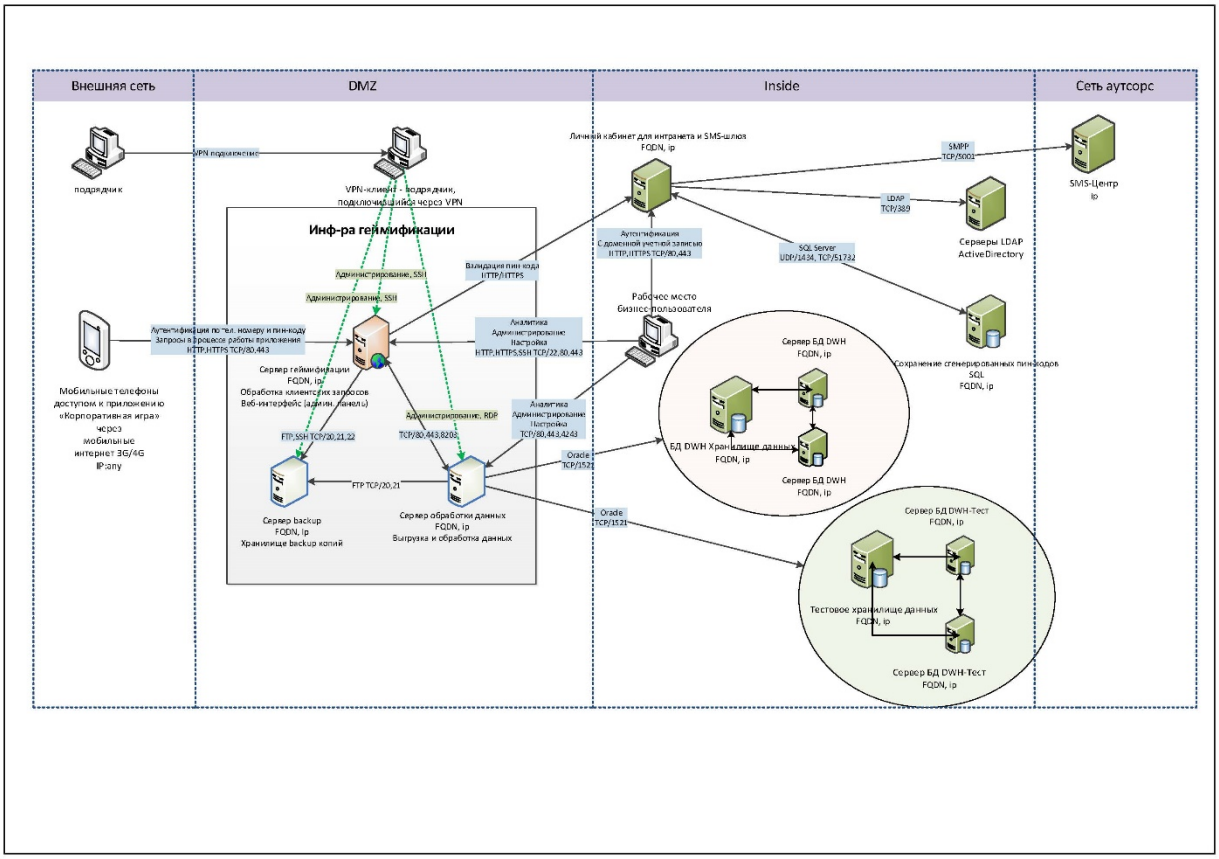

1. В целях безопасности убрать взаимодействие мобильного устройства с сервером геймификации по протоколу HTTP, оставить разрешенным только HTTPS по 443 порту.
2. Аналогично с рабочим местом бизнес-пользователя. Все запросы и доступы на сервера аутентификации, геймификации и сервера обработки данных должны идти через HTTPS.
3. Хочется отметить, что у бизнес-пользователя, а я подозреваю некого аналитика, слишком много привилегий для работы с серверами геймификации и обработки данных. Оставить только подключение через браузер по протоколу HTTPS для получения информации , которая доступна только для чтения.
4. Между сервером обработки данных и бэкап серверов проработать обмен более безопасный, нежели как в схеме FTP. В качестве решения могут подойти FTPS (FTP+SSL) или SFTP (SSH FTP) + задействовать кастомный порт.
5. Для подрядчиков лучше всего использовать SSH ключи для индентификации при администрировании linux систем.
6. Для администрирования подрядчиками windows server я бы проработал реорганизацию данного сервиса. К примеру, из DMZ данный сервер обработки данных убрать в инсайд. А в дмз поставить шлюз RDG (Remote Desktop Gateway) с установленным SSL сертификатом.
7. Пересмотреть порты для подключения к серверам баз данных. В идеале настроить их на кастомный с возможностью шифрования трафика.
8. В аутсорсной сети есть SMS центр, который использует 5001 порт. Лучше выбрать кастомный порт.
9. На сервере обработки данных и на контроллере домена очень вероятно можно найти персональные данные. А согласно приказу ФСТЭК №21 от 18.03.2013 г. , постановлению Правительства РФ №1119, 149-ФЗ и 152-ФЗ защита таких данных должна осуществляться должным образом – с использованием антивирусной защиты, систем обнаружения вторжений, анализ защищённости ПДН и разграничением прав доступа к данным, в идеале с использованием IDM систем).