1. **Описание системы:**

Система предназначена для доступа внешнего клиента к ресурсу компании для совершения каких-либо действий, в том числе:

* Регистрация в системе;
* Заполнение анкеты (ввод данных о себе) + загрузка файла с фото;
* Поиск каких-либо данных в системе;
* Вход/выход из аккаунта;
* Изменение пароля от своей учетной записи.

Доступ клиента осуществляется через браузер (стандартный web-доступ).

1. **Описание инфраструктуры системы:**
2. Состоит из двух сегментов: ДМЗ и внутренняя сеть.
3. Во внутренней сети функционирует CRM-система. Развернута на виртуализации (указание конкретного решения на ваш выбор). Основное назначение CRM – хранение клиентской информации.
4. Часть системы в DMZ отвечает за логику обработки запросов при доступе клиента к информации, расположенной в CRM; реализация функционала, описанного в п. 1 (Описание системы).
5. В сети компании присутствуют стандартные инфраструктурных сервисы Active Directory, почтовый сервис, DNS, DHCP, NTP



1. **Задачи**
2. Детализировать сегмент c CRM-системой предложив свой вариант архитектуры (например, балансировщик, frontend, backend, СУБД и т.д.).

Межсетевой экран - UserGate

Балансировщик - **Apache Storm, Apache kafka**

**Frontend – Angular, View, React**

**Backend - Битрикс24**

**Субд – Oracle или MySQL**

1. Детализировать сегмент ДМЗ указав какие компоненты должны быть вынесены в данный сегмент (например, балансировщик, frontend, backend, СУБД и т.д.).

Пограничный маршрутизатор -

Межсетевой экран – UserGate

Балансировщик нагрузки – Apache Storm, Apache kafka

1. Организовать взаимодействие между ДМЗ и внутренней сетью с учетом минимизации рисков несанкционированного доступа к внутренней сети.

ZeroTrust, NGFW, IPS/IDS

1. Дополнить схему сегментом внутренних пользователей и предложить вариант доступа к CRM.
2. На схеме следует учесть:
   1. Сетевые сегменты, если требуется разделение указать явно
   2. Информационные потоки – отразить стрелками указывающими направление соединения (инициатор -> приемник);
   3. Порты и протоколы в легенде;
   4. Компоненты системы согласно задачам п.1-2;
   5. Сегмента СЗИ и интеграции системы с ним.
   6. Можно добавлять компоненты на схеме по своему желанию, если это поможет повысить защищенность системы.
3. При проектировании системы и средств защиты бюджет не учитывать. Стек технологий для выполнения задания – на Ваш выбор.
4. **Для каждой подсистемы каждого компонента СRM системы предложить меры защиты как встроенные, так и наложенные, отразить можно в произвольной форме (значки на схеме, текстом и т.д.).**

**Подсистемы ИБ**

* подсистема сетевой безопасности
* подсистема контроля и управления доступом
* подсистема регистрации и учета
* подсистема обеспечения целостности
* подсистема защиты от вредоносного программного обеспечения (кода)
* подсистема криптографической защиты
* подсистема контроля защищенности
* подсистема безопасной интеграции
* подсистема безопасности среды виртуализации