1. **Описание системы:**

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

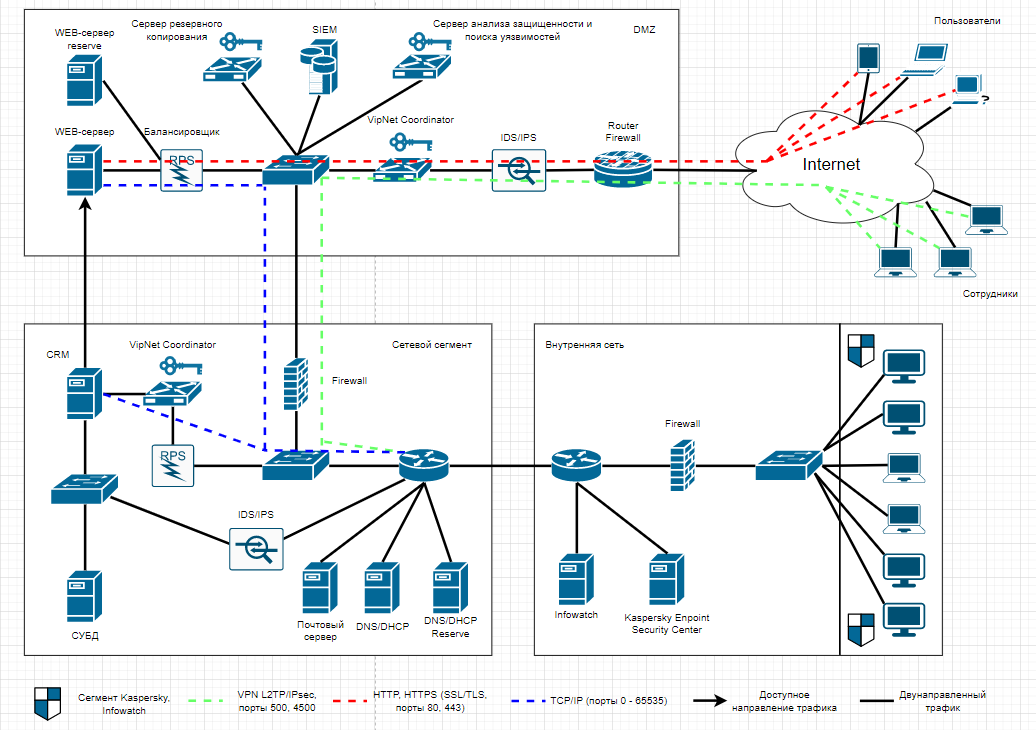
* Регистрация в системе;
* Заполнение анкеты (ввод данных о себе) + загрузка файла с фото;
* Поиск каких-либо данных в системе;
* Вход/выход из аккаунта;
* Изменение пароля от своей учетной записи.

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.).
3. Детализировать сегмент ДМЗ указав какие компоненты должны быть вынесены в данный сегмент (например, балансировщик, frontend, backend, СУБД и т.д.).
4. Организовать взаимодействие между ДМЗ и внутренней сетью с учетом минимизации рисков несанкционированного доступа к внутренней сети.
5. Дополнить схему сегментом внутренних пользователей и предложить вариант доступа к CRM.
6. 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.
7. При проектировании системы и средств защиты бюджет не учитывать. Стек технологий для выполнения задания – на Ваш выбор.



**Ко всей информационной системе я бы применил модель безопасности ZeroTrust (если мы рассматриваем приоритет безопасности над удобством пользования).**

1. Подсистема сетевой безопасности

**Встроенные меры защиты:**

Механизм аутентификации, ограничения на доступ с неразрешенных IP-адресов и сетей.

**Наложенные меры защиты:**

Мониторинг сетевой активности с помощью IDC/IPS, Vipnet IDS NS, Siem системы с настроенными правилами корреляции на сбор логов с DNS/DHCP, СУБД, Web-сервера, IDS/IPS, Почтового сервера, CRM.

1. Подсистема контроля и управления доступом

**Встроенные меры защиты:**

Разграниченный контроль доступа с ролевой моделью к объектам сетевой инфраструктуры (например доступ к DNS/DHCP, Почтовому серверу есть только у админов, сетевых инженеров и сотрудников ИБ)

Доступ к Infowatch, Kaspersky, Vipnet, SIEM только у сотрудников ИБ.

Доступ к СУБД, CRM, Web-серверу только у администраторов CRM системы.

Сетевой доступ до перечисленных выше объектов настраиваетcя политиками прав доступа в AD.

**Наложенные меры защиты:**

Физический доступ к перечисленным выше объектам предоставляется только администраторам соответствующих отделов по магнитным картам, мультифакторная аутентификация, использование биометрии, системы мониторинга и регистрации событий.

1. Подсистема регистрации и учета

**Встроенные меры защиты:**

Логирование событий (входа/выхода в учетные записи сотрудников, изменения прав доступа, учет носителей информации, неудачные попытки входа в УЗ на узлах или почтовом сервисе) с последующей передачей на SIEM.

**Наложенные меры защиты:**

Бэкапы и анализ журналов событий

1. подсистема обеспечения целостности

**Встроенные меры защиты:**

Использование хэширования и цифровых подписей для проверки целостности данных, контроль сигнатур и версий компонентов CRM

**Наложенные меры защиты:**

Мониторинг изменений на уровне файловой системы, Pentest, проверка на отсутствие вредоносного ПО,физическая охрана СВТ и носителей информации, обеспечение целостности программных средств и обрабатываемой информации, периодическое тестирование СЗИ НСД, наличие бэкапа СЗИ НСД и серверной составляющей сетевого сегмента.

1. Подсистема защиты от вредоносного программного обеспечения (кода)

**Встроенные методы защиты:**

Проверка кода на наличие уязвимостей, анализ и классификация угроз и уязвимостей, штатное включение механизмов проверки подлинности.

**Наложенные меры защиты:**

Kaspersky Endpoint Security (с постоянным обновление сигнатурных баз, настройками доступа к сетевым ресурсам сегмента Internet), своевременное обновление систем, мониторинг обнаружения поведенческих аномалий.

1. Подсистема криптографической защиты

**Встроенные меры защиты:**

Использование криптографических протоколов и ключей, цифровые сертификаты, шифрование данных в БД и файловой системе.

**Наложенные меры защиты:**

Vipnet coordinator шифрует данные пользователей, поступающее на web сервер, с последующей передачей зашифрованного трафика на CRM, удаленное подключение сотрудников по SSH ключам, с отключенной аутентификацией по паролю, проведение pentest’a с применением перебора паролей и атак на криптографические протоколы.

1. Подсистема контроля защищенности

**Встроенные меры защиты:**

Централизованное управление политикой безопасности, проверка СЗИ НСД на соответствие стандартам защиты, управление правами доступа и ролями, системы проверки на отсутствие уязвимостей.

**Наложенные меры защиты:**

IDS/IPS, проведение тестирований на проникновение, мониторинг событий ИБ.

1. Подсистема безопасной интеграции

**Встроенные меры защиты:**

Проверка целостности и аутентификация внешних систем, штатное использование протоколов безопасности, контроль доступа к экспортируемым объектам и интерфейсам.

**Наложенные меры защиты:**

Управление рисками интеграций, мониторинг входящего и исходящего трафика данных, использование промежуточных агентов для фильтрации.

1. Подсистема безопасности среды виртуализации

**Встроенные меры защиты:**

Разделение ресурсов среды виртуализации, контроль доступа к виртуальным машинам и ресурсам, механизмы изоляции и ограничения на уровне хоста и гостевой ОС.

**Наложенные меры защиты:**

Настройка доступа к хостовой ОС, использование механизмов управления и контроля сетевых интерфейсов, проверка целостности имиджей виртуальных машин.