Лабораторная работа №2 «Разработка требований к корпоративной сети»

В соответствии с выбранной в ходе выполнения ЛР№1 темой, разработать требования к локальной вычислительной (корпоративной) сети организации (конфигурация сети):

1. **Ранг сети – одноранговая, многоранговая.**

Для организации ПАО «Московская Биржа», используется исключительно многоранговаясеть на основе архитектуры «клиент-сервер».

* В многоранговой сети все учетные записи пользователей, политики безопасности и права доступа управляются централизованно с контроллеров домена. Это является отраслевым стандартом для обеспечения безопасности и контроля в крупных компаниях.
* Иерархическая структура (Ядро - Распределение - Доступ) позволяет легко добавлять новые отделы, серверы и пользователей без коренной перестройки сети
* Позволяет реализовать строгую сегментацию сети. Критически важные серверы могут быть изолированы в отдельные сегменты (VLAN) с ограниченным доступом
* Специализированные серверы берут на себя основную вычислительную нагрузку, обеспечивая высокую скорость работы.

1. **Тип сети – проводная, беспроводная, смешанная.**

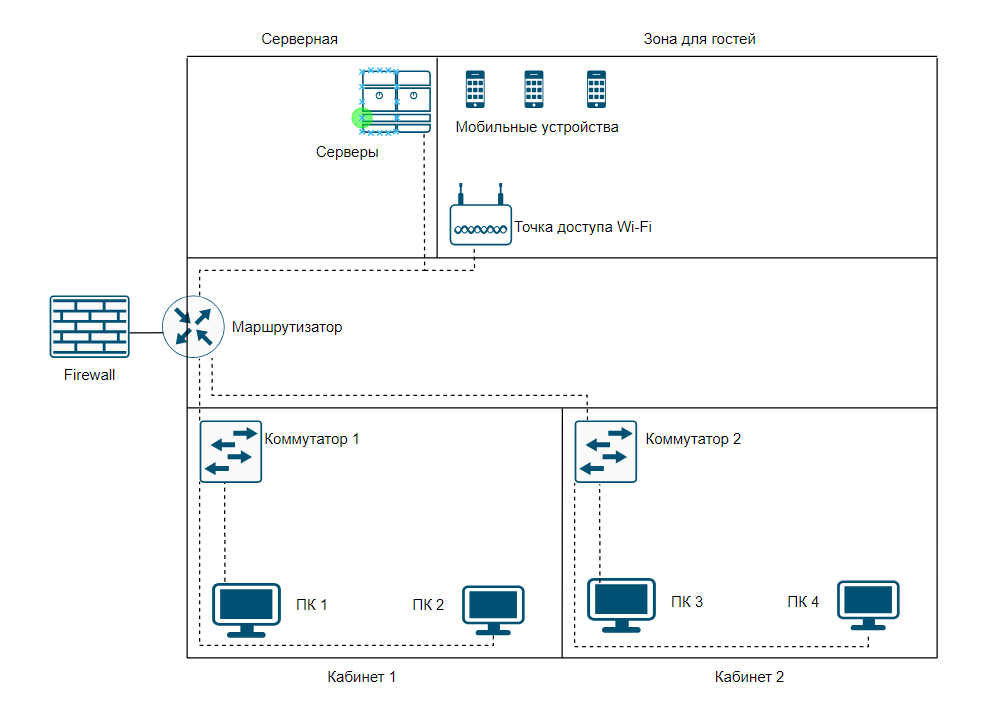
Проводная сеть (Ethernet) как основа:

* Высокая скорость и надежность, т.к. все стационарные рабочие места (трейдеры, аналитики, разработчики), серверные стойки и сетевая инфраструктура подключены с помощью проводных гигабитных и 10-гигабитныех соединений.
* Физическое подключение снижает риск несанкционированного доступа по сравнению с беспроводным каналом.
* Отсутствие помех и гарантированная полоса пропускания критически важны для торговых и аналитических систем.

Беспроводная сеть (Wi-Fi) как дополнение:

* Предоставление доступа для гостей, мобильных сотрудников (с планшетами/ноутбуками) в переговорных комнатах, зонах отдыха, а также для подключения вспомогательного IoT-оборудования.

1. **Схема узлов сети – с наложением на планы зданий и помещений, занимаемых организацией.**



1. **Группы и роли пользователей.**

* Администраторы безопасности - Доступ к системам мониторинга и управления безопасностью (SIEM, межсетевые экраны).
* Продакт-менеджер
* Аналитики срочного рынка
* Sales-менеджер
* Маркетмейкеры
* Гости

1. **Права доступа пользователей и групп к узлам сети.**

* Администраторы безопасности - Доступ к системам мониторинга и управления безопасностью (SIEM, межсетевые экраны).
* Продакт-менеджер - Пользователи с доступом к критическим торговым системам и данным в реальном времени.
* Аналитики срочного рынка - Пользователи с доступом к аналитическим и историческим данным, системам моделирования.
* Sales-менеджер - Пользователи с доступом к CRM-системам, базам клиентов, тарифным моделям.
* Маркетмейкеры -  Доступ к выделенным сегментам сети для подключения торговых роботов и серверов, размещенных вне площадки биржи
* Гости - Временные пользователи с доступом только в Интернет через гостевую сеть Wi-Fi.

1. **Политики безопасности.**

* Политика контроля доступа
  + Пользователям предоставляется доступ только к тем сетевым ресурсам и данным, которые необходимы для выполнения их прямых должностных обязанностей.
  + Для всех сотрудников – обязательное использование двухфакторной аутентификации при входе в домен и критически важные системы. Для внешних маркет-мейкеров – аутентификация на основе сертификатов
  + Ежеквартальная проверка членства в группах и предоставленных прав доступа для выявления несоответствий
* Политика сетевой безопасности
  + Обязательное использование VLAN для логической изоляции сегментов. Запрет на прямое взаимодействие между VLAN без явной необходимости, контролируемой межсетевыми экранами
  + Все входящие и исходящие данные проходят через каскад межсетевых экранов с включенной функцией IPS/IDS
  + Обязательное использование VPN для всех удаленных подключений. Использования протоколов HTTPS, TLS для внутреннего трафика.
* Политика использования беспроводных сетей
  + Гостевая сеть Wi-Fi должна быть полностью изолирована от корпоративной сети на аппаратном уровне
  + Для корпоративного Wi-Fi используется WPA2-Enterprise или WPA3 с аутентификацией через RADIUS-сервер, интегрированный с Active Directory.
  + Обязательное ведение логов о подключениях к Wi-Fi для возможности расследования инцидентов.
* Политика резервного копирования и восстановления
  + Правило 3-2-1: Хранить 3 копии данных, на 2 разных типах носителей, 1 копия — в другом здании).
  + Ежеквартальное проведение учебных восстановлений данных из резервных копий для проверки их целостности и отработанности процедур.
* Политика реагирования на инциденты
  + Любой сотрудник, обнаруживший подозрительную активность (например, фишинг, неработающий антивирус), обязан немедленно сообщить в слуюжу поддержки
  + Существует пошаговый план действий для администраторов при обнаружении разных типов инцидентов
  + После ликвидации инцидента проводится обязательный разбор причин и принимаются меры по недопущению его повторения.
* Политика для мобильных и персональных устройств
  + Личные устройства сотрудников (ноутбуки, смартфоны) не имеют права подключаться к проводной корпоративной сети
  + Для личных устройств возможен доступ только к гостевой сети Wi-Fi
* Политика физической безопасности
  + Серверные комнаты и телекоммуникационные шкафы должны быть оборудованы системами контроля доступа
  + Запрещено подключение к сети любых неподконтрольных IT-отделу устройств без предварительной проверки и регистрации.