ПРОЕКТИРОВАНЕ СИСТЕМЫ БЕЗОПАСНОСТИ КОВОРКИНГА ДЛЯ ФРИЛАНСЕРОВ

РЕДИНОВ ДМИТРИЙ МАКСИМОВИЧ

МИНАЕВА МИРРА ДМИТРИЕВНА

**1. Общее описание:**

Главная цель сети — обеспечить надёжное, быстрое и безопасное подключение всех пользователей к Интернету с полной изоляцией трафика между клиентами, а также предоставить сотрудникам и администраторам возможность безопасного управления оборудованием и сервисами.

Основные задачи проекта:

* Организация стабильного высокоскоростного Wi-Fi-доступа для фрилансеров и гостей коворкинга.
* Создание выделенной служебной инфраструктуры для сотрудников и систем видеонаблюдения.
* Обеспечение защиты данных и предотвращение несанкционированного доступа.
* Внедрение системы авторизации пользователей и управления доступом.
* Повышение отказоустойчивости сети за счёт резервирования оборудования и каналов связи.

Проектная сеть должна быть удобной для пользователей, легко управляемой, безопасной и готовой к масштабированию при увеличении количества клиентов.

**2. Логическая схема сети:**

Для разработки логической схемы нужно выделить основные группы пользователей и их роли, определите их потребности в обмене данными и доступе к ресурсам.

**Первая** группа **-** это гости, фрилансеры основные пользователи коворкинга. Которым требуется доступ в интернет и, возможно, к общим принтерам. Их ключевое требование - полная изоляция друг от друга.

Им нужно: Интернет (основной ресурс), Общие принтеры (по необходимости).

Запрещено: Любой доступ к другим VLAN, включая других фрилансеров.

**Вторая** группа **-** это администраторы, сотрудники коворкинга (менеджеры, бухгалтер, техподдержка). Им нужен доступ к управляющим системам, финансам, камерам и оборудованию

Им нужно: Интернет, Сервер управления (если есть), Система контроля доступа, IP-камеры, Финансовые сервисы, Принтеры.

И **третья группа -** отдельная служебная сеть всех сетевых устройств (коммутаторы, точки доступа, маршрутизатор, камеры). Эта сеть должна быть строго изолирована от пользовательских.

Далее нужно определить требования к подключению:

**Количество пользователей в каждом отделе и количество сетевых устройств:**

* Гости: 200 рабочих мест.
  + Устройства: 300-400 устройств (у каждого фрилансера может быть ноутбук, телефон и/или планшет).
* Администрация: допустим, 10 сотрудников.
  + Устройства: 15-20 устройств (ПК, телефоны, служебные ноутбуки).
* Служебная сеть:
  + Устройства: 30-50 устройств (коммутаторы, точки доступа, камеры, маршрутизатор).

Итого: примерно 470 активных сетевых устройств

**Затем нужно определить необходимости в беспроводном доступе и мобильности:**

* Wi-Fi является основным и единственным способом подключения для фрилансеров. Проводные розетки могут отсутствовать как класс.
* Мобильность критически важна. Пользователи должны свободно перемещаться по пространству коворкинга без потери соединения (требуется бесшовный роуминг)

После успешного планирования и проработки предметной области, можно приступить к проектированию логической технологии:

**Схема VLAN для сегментации сети по отделам и функциям:**

|  |  |  |  |
| --- | --- | --- | --- |
| VLAN ID | Имя VLAN | Описание | Подсеть |
| **10** | MGMT | Управление сетевым оборудованием | 10.10.10.0/24 |
| **20** | ADMIN | Сотрудники администрации | 10.10.20.0/24 |
| **50** | SERVICES | Офисное оборудование | 10.10.50.0/24 |
| **100** | FREELANCERS | Основные клиенты (фрилансеры) | 10.10.100.0/24 |

**Общение VLAN:**

* VLAN 100 (Фрилансеры):
  + Изолирован: не может общаться с другими устройствами в том же VLAN 200.
  + Доступ: имеет доступ только к VLAN 50 (Принтеры) и в Интернет. Весь трафик между фрилансерами блокируется на уровне коммутатора (функция Private VLAN или изоляция на точке доступа).
* VLAN 20 (Admin):
  + Доступ: имеет доступ ко всем другим VLAN (для управления) и в Интернет.
* VLAN 50 (Сервисы):
  + Доступ: Доступен из VLAN 100 (Фрилансеры) и VLAN 20 (Admin) по определенным, ограниченным портам (например, 9100 для печати).

**Логическая схема:**

Изображение выглядит как текст, диаграмма, снимок экрана, рукописный текст

Содержимое, созданное искусственным интеллектом, может быть неверным.

**3. Физическая инфраструктура:**

**Выбор технологий и протоколов:**

**Внутренняя маршрутизация:**

Между VLAN маршрутизация на L3 (SVI) в паре с централизованным фаерволом.

Самый оптимальный вариант сценария:

* Два ядра/агрегации (стек/MLAG). Между агрегаторами и внешним маршрутизатором — несколько ссылок (LACP).
* Используем **динамический протокол OSPF (single area)** для внутренних маршрутов.
* Причины: OSPF автоматически перенастроит маршрутизацию при отказе ссылки/устройства, проще масштабируется, легче поддерживать множественные агрегационные устройства и VRF при необходимости.
* Если планируем 2+ ISP — маршрутизатор/edge использует **BGP** с провайдерами; внутри сети — OSPF.

**Политики безопасности и контроль доступа:**

* Меж-VLAN трафик идёт через L3-коммутатор + ACL на SVI/фаервол (принцип «deny by default», затем белые правила).
* Для тонкой сегментации (per-client isolation) комбинируем: Private VLAN / AP client-isolation + RADIUS Dynamic VLAN assignment (если нужно назначать клиентам отдельные VLAN по RADIUS).

Итог: **L3-агрегацию + OSPF** внутри (два агрегатора/ядра в HA/стеке). На границе — высокопроизводительный фаервол/маршрутизатор (с поддержкой BGP при наличии 2 ISP). Это и поможет обеспечить бесперебойную сеть, а также разграничить права внутри сети.

**Беспроводная сеть:**

Разворачиваем Wi-Fi 6 (802.11ax) как основу. Если бюджет и локальные правила позволяют, использовать Wi-Fi 6E (6 GHz) для разгрузки 2.4/5 GHz. Это оптимальный подход для условий коворкинг - кафе. Оставляем архитектуру «AP-ready» для лёгкого перехода на Wi-Fi 7 (802.11be) в будущем, тк Wi-Fi 7 еще не подходит для такого потока клиентов.

Аутентификация / авторизация:

* Admin/Персонал/Устройства: WPA3-Enterprise (802.1X) + RADIUS (EAP-TLS или EAP-PEAP с MSCHAPv2 если нет PKI). Рекомендовано — EAP-TLS (сертификаты) для максимальной безопасности.
* Freelancers (основной клиентский SSID): Сaptive portal + OAuth (соцсети) для удобства регистрации. В этом случае backend captive portal делает динамическое назначение VLAN через RADIUS (RADIUS Reply — Tunnel/Framed-VLAN) или возвращает токен, а сеть помещает пользователя в VLAN FREELANCERS.

Для изоляции клиентов используется Client-isolation на SSID + при возможности Private VLAN на коммутаторе/AP для блокировки L2/L3 общения клиентов между собой. Дополнительно — сетевые ACL на SVI чтобы запретить межклиентский трафик.

**Нефункциональные требования**

**Производительность:**

### Внешние/магистральные каналы (internet) - следует выбрать 1 Gbps симметричный (основной) + резервный канал от второго ISP (можно 200–500 Mbps) в режиме failover/ECMP/BGP. Тк 200 рабочих мест это пиковое потребление (стриминг, загрузки) может потребовать высокий агрегированный throughput; 1 Gbps — минимально практичный старт. Возможность быстрого апгрейда до 2.5 / 5 Gbps по мере роста.

Внутренняя магистраль:

* Core / aggregation uplinks: минимум 10 Gbps SFP+ между ядром и агрегацией.
* Aggregation access uplinks: 10 Gbps (SFP+) или, при распределённой модели, LACP 2×10G. Для участков с большим количеством AP/интенсивным трафиком — использовать 25 Gbps на ядре (если планируете масштаб и heavy traffic).
* Access AP uplinks: многопортовые PoE-коммутаторы должны иметь 1 Gbps порты для обычных AP; для AP с multi-gig (Wi-Fi 6E/7) рекомендуется 2.5/5 Gbps порты на AP или multi-gig uplink на коммутаторе.

Порты: лучше использовать multi-gig (2.5G/5G) или 1G с запасом, тк современные AP при высокой плотности и при поддержке нескольких радиочастот лучше работают на multi-gig uplink.

**Доступность:**

Для обеспечения стабильной работы сети коворкинга и предотвращения простоев необходимо предусмотреть систему резервирования и мониторинга оборудования.

Основная цель — гарантировать бесперебойный доступ пользователей к ресурсам сети и интернет-каналу даже при частичных отказах оборудования.

**Требуемая доступность элементов сети:**

* Для маршрутизатора, межсетевого экрана и коммутаторов ядра — не ниже **99,95 %** (допустимый простой не более 4 часов в год).
* Для коммутаторов доступа и точек беспроводного доступа — **99,9 %** (не более 9 часов простоя в год).

**Меры обеспечения отказоустойчивости:**

1. **Резервирование каналов связи.**  
   Следует предусмотреть подключение к двум независимым провайдерам интернет-доступа. При отказе основного канала переключение должно выполняться автоматически.
2. **Резервирование оборудования.**  
   Коммутаторы уровня агрегации объединяются в стек с функцией автоматического переключения при выходе из строя одного из устройств.  
   Маршрутизатор и межсетевой экран должны поддерживать режим высокой доступности (актив-резерв).
3. **Агрегация каналов.**  
   Между уровнями доступа и агрегации рекомендуется использовать объединение физических каналов (аналог протокола LACP), что повышает пропускную способность и защищает от обрыва отдельного линка.
4. **Резервирование сервисов авторизации.**  
   Сервера RADIUS и системы авторизации пользователей должны быть установлены в количестве не менее двух (основной и резервный) с синхронизацией данных.
5. **Питание и защита оборудования.**  
   Все активные устройства необходимо подключить к источникам бесперебойного питания (ИБП) с резервом времени не менее 10–15 минут.  
   В распределительных шкафах рекомендуется предусмотреть стабилизаторы напряжения и систему вентиляции.
6. **Мониторинг.**  
   В сети должна быть развернута система централизованного мониторинга, которая отслеживает состояние оборудования, нагрузку на каналы и своевременно уведомляет администратора о сбоях.

**Требования к оборудованию**

Для коворкинг кафе стоит использовать современное управляемое сетевое оборудование, обеспечивающее поддержку всех необходимых технологий сегментации, безопасности и беспроводного доступа. Ниже приведены основные характеристики для каждого уровня сети.

**3.а. Коммутаторы доступа**

Коммутаторы уровня доступа предназначены для подключения пользовательских устройств, точек беспроводного доступа и камер видеонаблюдения.

**Основные характеристики:**

* Количество портов — не менее **48 портов Ethernet 10/100/1000 Мбит/с** для подключения рабочих мест и точек доступа.
* Наличие не менее **4 портов 10 Гбит/с (SFP+)** для подключения к коммутаторам агрегации.
* Поддержка **питания по технологии PoE+ (IEEE 802.3at)**, обеспечивающей питание точек доступа и IP-телефонов.
* Общий энергетический бюджет PoE — не менее **800–1000 Вт** на коммутатор.
* Поддержка **виртуальных локальных сетей (VLAN, 802.1Q)** и приоритезации трафика (QoS).
* Наличие функций **быстрого согласования связей (RSTP/MSTP)** и **аутентификации пользователей (802.1X)**.
* Управляемость через веб-интерфейс и консоль, поддержка SNMP для мониторинга.
* Возможность объединения коммутаторов в стек для упрощения управления и повышения отказоустойчивости.

**3.б. Коммутаторы агрегации (ядра)**

Коммутаторы агрегации выполняют функции маршрутизации между VLAN, объединяют коммутаторы доступа и обеспечивают подключение к маршрутизатору и межсетевому экрану.

**Основные характеристики:**

* Пропускная способность не менее **640 Гбит/с**.
* Поддержка **портов 10/25 Гбит/с (SFP+)** для подключения оборудования уровня доступа.
* Наличие аппаратной поддержки маршрутизации по протоколу **OSPF**.
* Возможность объединения в стек или кластер с синхронизацией конфигурации.
* Поддержка механизмов **качественного обслуживания (QoS)**, **списков контроля доступа (ACL)** и **фильтрации трафика**.
* Наличие резервируемых блоков питания и вентиляторов.
* Поддержка **агрегации каналов (LACP)** и **резервирования соединений**.

**Функции:**

* Межвлановая маршрутизация (L3-интерфейсы для VLAN 10, 20, 50, 100).
* Обеспечение связи между сегментами ADMIN, FREELANCERS, MGMT и SERVICE.
* Передача трафика на маршрутизатор и межсетевой экран.

**3.в. Маршрутизатор и межсетевой экран**

Маршрутизатор и межсетевой экран (МСЭ) обеспечивают выход в Интернет, защиту от внешних угроз и разделение сетевых зон по уровням доступа.

**Основные характеристики:**

* Пропускная способность при включённых функциях фильтрации и контроля — не менее **2–3 Гбит/с**.
* Поддержка не менее **8 логических зон безопасности** (MGMT, ADMIN, FREELANCERS, SERVICES, CAMERAS, GUEST, DMZ, INTERNET).
* Наличие функций **межсетевого экрана, NAT, антивирусной фильтрации и системы предотвращения вторжений (IPS)**.
* Поддержка **VPN-соединений** (IPsec и SSL) для удалённого доступа сотрудников.
* Возможность организации режима **высокой доступности (актив-резерв)**.
* Поддержка журналирования событий и передачи логов на централизованный сервер.
* Наличие двух интерфейсов WAN для подключения к разным провайдерам и функции автоматического переключения при отказе.

**Функции:**

* Контроль и фильтрация межсетевого обмена между VLAN.
* Ограничение доступа пользователей к внутренним ресурсам.
* Организация безопасного выхода в Интернет.
* Поддержка авторизации пользователей через сервер RADIUS и Captive Portal.

**3.г. Точки беспроводного доступа**

Так как основным способом подключения пользователей к сети является Wi-Fi, особое внимание уделяется выбору точек доступа.

**Основные характеристики:**

* Поддержка стандарта **Wi-Fi 6 (802.11ax)**, а при возможности — **Wi-Fi 6E** (диапазон 6 ГГц).
* Поддержка функций **бесшовного роуминга (802.11k, 802.11v, 802.11r)**.
* Поддержка аутентификации по стандарту **WPA3-Enterprise** и интеграции с сервером RADIUS.
* Возможность организации гостевого доступа через **веб-портал с авторизацией через социальные сети**.
* Поддержка **изоляции клиентов** внутри одной беспроводной сети.
* Питание по PoE+ (до 30 Вт на устройство).
* Поддержка централизованного управления и обновления прошивок.

**Примерное количество:**  
Ориентировочно 20 точек доступа для покрытия всего пространства коворкинга с учётом плотности 15–20 клиентов на одну точку

**Требования к сетевой безопасности**

Сетевая безопасность является ключевым элементом инфраструктуры коворкинга, так как сеть используется большим количеством независимых пользователей. Необходимо обеспечить защиту оборудования, данных и сервисов от несанкционированного доступа как со стороны внешних источников, так и между пользователями внутри сети.

### Правила на межсетевом экране (МСЭ)

Межсетевой экран выполняет роль центрального средства защиты и разграничения доступа между VLAN.

Вся маршрутизация между сегментами должна проходить через МСЭ, где применяются следующие правила:

|  |  |  |  |
| --- | --- | --- | --- |
| **Источник** | **Назначение** | **Разрешённые порты/сервисы** | **Назначение** |
| VLAN 100 (Фрилансеры) | Интернет | 80, 443 | Доступ к внешним ресурсам |
| VLAN 100 (Фрилансеры) | VLAN 50 (Сервисы) | 9100 | Печать на общих принтерах |
| VLAN 100 (Фрилансеры) | VLAN 20, VLAN 10 | Запрещено | Полная изоляция клиентов |
| VLAN 20 (Администрация) | VLAN 10 (Управление) | 22, 443 | Администрирование оборудования |
| VLAN 20 (Администрация) | Интернет | 80, 443 | Общий доступ |
| VLAN 10 (Управление) | Все VLAN | По необходимости | Управление сетевыми устройствами |
| VLAN 50 (Сервисы) | VLAN 20, VLAN 100 | Только служебные порты | Печать, авторизация, камеры |

Все неиспользуемые и потенциально опасные порты должны быть закрыты.

Трафик между клиентами внутри VLAN 100 блокируется функцией «изоляции клиентов» (Client Isolation) и политикой Private VLAN.

**Политика доступа в Интернет**

Для различных категорий пользователей устанавливаются отдельные правила доступа в Интернет:

1. **Фрилансеры (гости коворкинга):**
   * Доступ предоставляется после авторизации через веб-портал (Captive Portal) или через социальные сети.
   * Пользователь получает динамический IP-адрес из VLAN 100.
   * Разрешён доступ только к внешним веб-ресурсам (HTTP, HTTPS).
   * Запрещён доступ к внутренним VLAN и локальным устройствам.
   * Время сессии может быть ограничено (например, 8 часов).
   * Применяется контентная фильтрация для блокировки вредоносных и нежелательных категорий сайтов.
2. **Сотрудники администрации:**
   * Доступ предоставляется без ограничений, но весь исходящий трафик проходит через антивирусную и контентную фильтрацию на уровне МСЭ.
   * Действия пользователей логируются в системе журналирования.
   * Разрешается подключение к внутренним ресурсам (сервер, камеры, система контроля доступа).
3. **Служебное оборудование (камеры, точки доступа, коммутаторы):**
   * Не имеет прямого выхода в Интернет.
   * Доступ разрешён только к внутренним сервисам (например, обновление прошивок с доверенных адресов).

### Безопасный удалённый доступ

Для удалённой работы сотрудников предусмотрено использование **VPN-подключения**.  
Применяется технология **IPsec VPN** или **SSL VPN** с двухфакторной аутентификацией.

**Основные требования:**

* Аутентификация пользователей через сервер RADIUS.
* Передача данных в зашифрованном виде (AES-256).
* Поддержка не менее 20 одновременных подключений.
* Автоматическое завершение неактивных сессий через заданный интервал времени.
* Журналирование подключений с фиксацией IP-адресов и времени входа.
* При подключении назначается IP-адрес из отдельного пула, не совпадающего с адресами локальных VLAN.
* Разрешается доступ только к VLAN 20 (администрация) и VLAN 10 (управление).

## Требования к подключению к Интернет

Для обеспечения надёжной связи и бесперебойной работы пользователей необходимо предусмотреть основные и резервные каналы подключения к Интернету.

1. **Основной канал:**
   * Пропускная способность — не менее **1 Гбит/с** симметрично.
   * Возможность увеличения до **2,5–5 Гбит/с** без модернизации оборудования.
   * Канал должен предоставляться оператором с гарантией SLA не ниже **99,95 %**.
2. **Резервный канал:**
   * Пропускная способность — не менее **300–500 Мбит/с**.
   * Используется для автоматического переключения при отказе основного.
   * Подключается через независимого провайдера связи.
3. **Отказоустойчивость и маршрутизация:**
   * Автоматическое переключение между каналами выполняется с помощью динамической маршрутизации (OSPF или BGP).
   * Межсетевой экран должен поддерживать резервирование WAN-интерфейсов и синхронизацию таблиц соединений при переключении.
4. **Мониторинг каналов:**

* Система мониторинга должна контролировать доступность обоих каналов, фиксировать скорость передачи данных и уведомлять администратора при сбоях.