Облачные технологии

**IaaS (Infrastructure as a Service)** — это модель использования облачных сервисов, где компания арендует у провайдера вычислительные мощности его IT-инфраструктуры.

Некоторые элементы IaaS:

* **Виртуальные серверы**. На них можно хостить сайты, размещать CRM или ERP-систему компании и так далее.
* **Облачные хранилища данных**. Их можно масштабировать по мере необходимости.
* **Сетевые ресурсы**. Это виртуальные сети, маршрутизаторы и балансировщики нагрузки, которые повышают безопасность и защищают от перегрузок.
* **Системы резервного копирования и восстановления**. Они защищают данные клиента в случае сбоев.
* **Службы безопасности**. Это межсетевые экраны, шифрование данных и другие инструменты для защиты от несанкционированного доступа к данным и других угроз.

Услуга основана на принципе виртуализации: провайдер арендует не само «железо», а только его мощности. Он создаёт виртуальные серверы на базе физических и предоставляет своим клиентам доступ к ним.

## Преимущества IaaS:

* **Экономия**. Арендовать мощности у провайдера дешевле, чем покупать оборудование.
* **Масштабируемость**. Технология позволяет оперативно увеличивать или сокращать ресурсы в зависимости от текущих потребностей бизнеса.
* **Гибкость**. При необходимости можно развёртывать разнообразные операционные системы и ПО на виртуальных машинах, получая ещё больше мощности и производительности.
* **Доступность**. Платформы как услуги с хорошей репутацией гарантируют безотказность и высокий аптайм облачных сервисов, что крайне важно для стабильной работы бизнеса.
* **Управление и контроль**. Компании сохраняют контроль над собственными данными и приложениями, в то время как провайдеры управляют исключительно инфраструктурой.

IaaS подходит для различных задач, среди которых: развёртывание в облаке корпоративной инфраструктуры, хостинг сайтов и приложений, разработка и тестирование ПО, хранение и обработка больших объёмов данных, резервное копирование данных.

# Облачные сервисы AWS VPC и VNet

AWS VPC (Virtual Private Cloud) — это сервис облачных вычислений от Amazon Web Services (AWS), который позволяет создавать логически изолированную виртуальную сеть для запуска ресурсов в облаке

Некоторые возможности сервиса:

* **Настраиваемая конфигурация сети**. Пользователь имеет полный контроль над виртуальной сетевой средой, включая выбор диапазона IP-адресов, создание подсетей и настройку таблиц маршрутов и сетевых шлюзов.
* **Улучшенная безопасность**. VPC предоставляет такие функции, как группы безопасности и списки контроля доступа к сети, для фильтрации входящего и исходящего трафика на уровне экземпляра и подсети.
* **Гибкость подсетей**. В рамках VPC можно создавать несколько подсетей, каждая из которых может быть изолирована и доступна в интернете по-разному.
* **Поддержка VPN**. VPC позволяет подключать виртуальную сеть к удалённым сетям с помощью безопасных и зашифрованных VPN-соединений.
* **Интеграция с сервисами AWS**. VPC интегрирован с такими сервисами, как Amazon EC2, RDS и Lambda, обеспечивая безопасный и лёгкий доступ к этим ресурсам в виртуальной сети.

Azure Virtual Network (VNet) — это сервис Microsoft Azure, который позволяет создавать изолированную сетевую среду в облаке для безопасного взаимодействия ресурсов Azure друг с другом, с интернетом и локальными сетями.

Некоторые возможности сервиса:

* **Проектирование собственных сетевых топологий**. В рамках VNet можно создавать несколько подсетей с уникальными диапазонами IP-адресов.
* **Обеспечение безопасности и шифрования**. Azure VPN Gateway обеспечивает безопасные зашифрованные соединения между VNet и локальными сетями, поддерживая соединения типа «сайт к сайту» и «точка к сайту».
* **Интеграция с другими сервисами Azure**. VNet интегрируется с такими сервисами, как Azure Load Balancer и Azure Firewall, обеспечивая комплексное сетевое решение.
* **Оптимизация затрат**. VNet позволяет контролировать трафик данных и эффективно использовать ресурсы внутри сети.

## Разница между AWS VPC и VNet:

* **Размещение подсетей**. Подсети AWS привязаны к зонам доступности AWS, в то время как подсети Azure специфичны для региона без ограничений по зонам доступности.
* **Модели безопасности**. AWS использует группы безопасности (состоятельные) и списки контроля доступа к сети (бессистемные), Azure использует группы безопасности сети (состоятельные).
* **Поддержка IPv6**. AWS VPC требует явного назначения блоков CIDR IPv6, в то время как Azure VNet упрощает процесс с интегрированной поддержкой IPv6.

# Настройка облачных маршрутизаторов

## Настройка Mikrotik CHR

Некоторые шаги для настройки Mikrotik CHR в облаке:

* Скачать образ CHR с официального сайта Mikrotik.
* Создать виртуальную машину на облачной платформе, выбрав в качестве источника загруженный образ.
* Настроить сеть: выбрать подсеть, к которой будет подключена машина, назначить IP-адрес интерфейсу.
* Настроить маршрутизацию: добавить шлюз по умолчанию, проверить работоспособность маршрута.
* Настроить DNS: указать адреса DNS-серверов.
* Проверить конфигурацию: проверить присвоенные IP-адреса и маршруты с помощью команд в консоли.

## Настройка VPN

Настройка VPN для облачного маршрутизатора (на примере Keenetic):

* Установить компонент IPsec VPN на обоих роутерах (один будет выступать в роли сервера, другой — клиента).
* Настроить сервер: добавить подключение в разделе подключений IPsec, включить опции ожидания подключения удалённого пира и восстановления туннеля при разрывах.
* Настроить клиент: добавить подключение, включить опцию автоподключения, заполнить поле «Удалённый шлюз» IP-адресом или доменным именем сервера.
* Проверить тоннель: если все настройки указаны верно, тоннель должен открыться, а статус подключения будет отражаться в странице «Другие подключения».

# Гибридные сети

**Гибридные сети** — это компьютерные сети, в которых используется более одного типа технологии соединения или топологии. Например, домашняя сеть, в которой для подключения компьютеров используются кабели Wi-Fi и Ethernet, — гибридная.

## Интеграция локальной и облачной инфраструктуры

Гибридный подход позволяет эффективно распределить нагрузку между локальными и облачными ресурсами. Например, локальные ресурсы могут использоваться для хранения и обработки конфиденциальных данных, а облачные — для хранения менее важных данных и обеспечения вычислительных мощностей.

Для интеграции локальной и облачной инфраструктуры в гибридных сетях применяются специальные технологии, которые позволяют создавать безопасные каналы связи и синхронизировать данные.

## Преимущества и недостатки

Преимущества гибридных сетей:

* Гибкость и масштабируемость бизнес-процессов.
* Увеличение доступности и надёжности при выполнении задач.
* Сокращение расходов на ИТ-инфраструктуру за счёт оптимизации использования ресурсов.

Недостатки гибридных сетей:

* Сложность управления безопасностью из-за нескольких точек доступа для атаки.
* Проблемы с контролем доступа к данным — необходимо убедиться, что все приложения и удалённые устройства имеют доступ только к нужным данным.

## Технологии и инструменты

Для построения гибридных сетей используются, например:

* **Виртуализация** — позволяет создавать виртуальное окружение для запуска приложений и операционных систем на локальных и облачных ресурсах.
* **Облачные API** — обеспечивают доступ к облачной инфраструктуре и позволяют управлять ею в соответствии с требованиями бизнеса.
* **Платформы контроля и управления** — позволяют управлять всей инфраструктурой в единой управляемой среде.
* **Автоматизация процессов** — ускоряет и упрощает задачи управления, деплоя и мониторинга.