

Фреймворк построения архитектуры организации (Zachman Framework)

	Данные ЧТО	Функции КАК	Размещение, сеть ГДЕ	Люди КТО	Время КОГДА	Мотивация ЗАЧЕМ
Сфера действия, контекст	Бизнес-цели: доход, рост, поиск новых возможностей, новых поставщиков Товары: доставка продуктов/товаров, IPO	Обработка заказов, доставка продуктов, работа с клиентами и сотрудниками	Присутствие в городах и странах, целевая аудитория (по географическому признаку). Сетевая и облачная инфраструктура	Целевая аудитория - клиенты, сотрудники, поставщики, инвесторы. Заинтересованные стороны: банки, налоговая, таможня	Время: обработки заказа, его сборки, его доставки. График работы сотрудников. Время реакции на непредвиденные ситуации, выход на IPO	Доход (прибыльность), развитие, привлечение и удержание клиентов, создание новых рабочих мест
Бизнес-модель	Данные клиентов (ПДн), каталог товаров, данные о заказах, данные о сотрудниках (ПДн), отчеты	Прием и обработка заказов, управление клиентами и сотрудниками, финансовые операции, ИБ, закупка товаров	Расположение складов, зоны доставки, местоположение клиентов и курьеров, маршруты доставки	Клиенты, сотрудники: отдел ИТ и ИБ, отдел работы с заказчиками и клиентами, отдел доставки и т.п.	Время: обработки заказа, его сборки, его доставки. Время реакция на запросы клиента и на непредвиденные ситуации	Увеличение клиентской базы, оптимизация логистики, снижение издержек, защита ПДн, выполнение требований регуляторов
Системный проект	Модель данных: структура БД. Внешний интерфейс сервисов: определение Rest API. Определение различных бизнес процессов и их жизненного цикла	Микросервисная архитектура, наличие REST API для взаимодействия, аутентификация, авторизация, интеграция с внешними сервисами. Политики безопасности	Облачная инфраструктура, балансировка нагрузки, создание резервных серверов	Пользователи приложения, персонал: курьеры, операторы, технический персонал: администраторы, служба ИБ.	Сценарии использования, логирование, масштабирование, производительность	Обеспечение конфиденциальности, доступности, целостности, высокой производительности
Технический проект	Используемые: сервера БД (репликационные и нет), среда для выполнения кода, очереди сообщений, средства для аутентификации, для логирования и мониторинга	Сервисы: работа с каталогом продуктов, заказами, курьерами, платежами. Механизмы аутентификация, авторизации, криптографии, безопасность	Серверы, виртуальные машины, docker-контейнеры, kubernetes	Разработчики, тестировщики, UIX специалисты, DevOps инженеры, системные администраторы, сотрудники ИБ	Waterfall модель разработки, спринты, выпуск новых версий, автоматическое тестирование, развертывание, мониторинг и тех.поддержка 24/7	Разработка, тестирование, развертывание, тех.поддержка. Выпуск новых версий
Компоненты	Схема БД, диаграммы структуры сервисов, их поведения, конфигурационные файлы	Код на языке разработки (Go, Rust, C++, F#, TypeScript), верстка, скрипты	Сервисы, docker-контейнеры, kubernetes	Программисты, верстальщики, администраторы, DevOps-инженеры, специалисты по ИБ	Конфигурирование, логирование, обновление, устранение неполадок	Реализация требований/задач, обновление, поддержка работоспособности
Работа, функционирование	Реальные данные, используемые в приложении: товары, заказы, клиенты, сотрудники, поставщики, поставки, платежи и т.п.	Отправка заказа, получение его статуса, получение информации о курьер, взаимодействие с операторами	Стационарный компьютер, ноутбук, мобильное устройство клиента	Клиент, курьер, оператор	Время заказа - время доставки	Возможность заказать и получить заказ, разнообразие ассортимента товаров

## Фреймворк корпоративной архитектуры безопасности (SABSA)

	Данные ЧТО	Функции КАК	Размещение, сеть ГДЕ	Люди КТО	Время КОГДА	Мотивация ЗАЧЕМ
Contextual	Безопасность бизнеса с точки зрения целей организации. Учет специфики товаров разных категорий (пищевые и т.п.). Взаимодействие с поставщиками	Архитектура бизнеса с учетом требований ИБ. Риск-ориентированный подход с учетом требований регуляторов и бизнеса. Определение приоритетов и уровней риска	Распределенная структура организации, работа с удаленными и мобильными (перемещающимися) сотрудниками	Заинтересованные стороны. Участники бизнес-процессов: клиенты, поставщики, курьеры, другие сотрудники	Непрерывность процессов обеспечения бизнеса и ИБ	Непрерывность бизнеса: бесперебойное обслуживание клиентов. Минимизация рисков ИБ в работе организации. Выход на IPO. Расширение бизнеса
Conceptual	Архитектура организации (бизнеса) с учетом стремления к расширению и выходу на IPO	Планирование процессов ИБ с учетом ранее выявленных инцидентов ИБ. Автоматизация процессов ИБ	Архитектура организации с учетом распределенной структуры и обеспечения ИБ. Взаимодействие с внешними субъектами	Сотрудники организации (курьеры, другие сотрудники), поставщики, клиенты, регуляторы ИБ	Планирование деятельности в области ИБ	Стратегический подход в области ИБ: снижение угроз ИБ, обеспечение безопасности и непрерывности бизнес-процессов, соответствие требованиям регуляторов.
Logical	Модель организации: финансовая, бизнес, технологическая. Организационная структура организации	Системы и сервисы, относящиеся к ИБ: аутентификация, авторизация, управление доступом, криптография, защита ПДн и т.д..	Топология расположения сервисов. Ролевая модель согласно структуре организации. Управление доступом. Доменная модель	Роли, пользователи, права, матрица доступа, принцип минимальных привилегий	Процессы обеспечения ИБ согласно принятым планам	Создание политики ИБ. Стремление к защите бизнес-процессов. Исполнение требования законодательства. Соответствие международным стандартам.
Physical	Структура (модель) данных и сами данные. Обработка данных с учетом требования ИБ. Инфраструктура: ПО, железо, сетевые устройства и коммуникации	Управление доступом и механизмами ИБ: физический доступ, видеонаблюдение, СКУД, сетевое оборудование, антивирусное ПО, межсетевая защита, криптография и т.д.	Топология сети и сетевых устройств. Реализация архитектуры. Развёртывание сервисов и систем.	Сотрудники организации, клиенты, поставщики, сотрудники провайдера.	Процессы обеспечения ИБ и контроль за ними	Регламенты и инструкции по обеспечению ИБ и контроль за ними
Component	Данные, разделенные на категории. Конфигурационные данные (настройки) ПО, железа, средств защиты	Средства защиты информации, криптографические средства, VPN, антивирусы, IDS/IPS, firewall и т.д.	Микросервисы, процессы, потоки данных, протоколы взаимодействия, логи, конфигурация	Аутентификация, авторизация, роли, пароли, ACL, УЗ	Задачи обеспечения ИБ внутри системы и при взаимодействии с ней извне	Исполнение требований, политик, регламентов ИБ с целью защиты бизнеса. Положительный аудит для IPO
Operational	Непрерывность деятельности, соблюдение необходимого уровня ИБ	Реализация и поддержка процессов ИБ. Взаимодействие с подразделениями, обучение пользователей	Захиста инфраструктуры: сеть, сервисы, сайты, мобильные приложения	Работа с УЗ пользователей системы. Защита данных пользователей системы	Время отслеживания и реагирования на инциденты ИБ. Время на восстановление	Безопасность работы бизнес-процессов. Безопасность данных пользователей.