Проект "ИТ Архитектура"

План реализации проекта "ИТ-архитектура"

Оглавление

5.2. Тестирование интеграций между системами.
5.3. Тестирование аварийного восстановления.
5.4. User Acceptance Testing (UAT).
5.5. Обучение пользователей.
5.6. Корректировка конфигураций по результатам тестирования.
5.7. Результат этапа 5.

6. Этап 6: Переход в Промышленную Эксплуатацию (Go-Live) и Поддержка
6.1. Go-Live Plan.
6.2. Планирование и выполнение перехода на новую инфраструктуру.
6.3. Активное сопровождение в начальный период после перехода.
6.4. Обучение администраторов/пользователей.
6.5. Передача документации и знаний службе поддержки (ITSM).
6.6. Запуск регулярных процессов мониторинга, резервного копирования, обновлений.
6.7. Post-Implementation Review (PIR).
6.8. Передача в эксплуатацию.
6.9. Закрытие проекта.
6.10. Результат этапа 6.

7. Дополнительные общие аспекты
7.1. Управление проектом.
7.2. Соблюдение стандартов и регулирования.
7.3. Устойчивость и экологичность.

Этап 1: Инициация и Планирование

Цель: Определить рамки проекта, собрать начальные требования, сформировать команду.

Деятельность:

1. Проведение стартовой встречи с заказчиком.
2. Определение целей, задач и критериев успеха проекта:
   2.1. Определение стратегических целей проекта:
      - Повышение надежности и отказоустойчивости ИТ-инфраструктуры предприятия.
      - Обеспечение необходимой производительности ИТ-систем для поддержки бизнес-процессов.
      - Создание масштабируемой архитектуры, поддерживающей будущий рост компании и развитие бизнеса.
      - Централизация управления ИТ и повышение эффективности ИТ-операций.
      - Повышение уровня информационной безопасности в соответствии с корпоративными и отраслевыми стандартами.
      - Обеспечение высокой доступности критически важных business-приложений (ERP, CRM, BI, почта).
      - Оптимизация затрат на ИТ-инфраструктуру в долгосрочной перспективе.
   2.2. Формулировка конкретных задач проекта:
      - Разработка целевой ИТ-архитектуры, охватывающая все 12 ключевых направлений (см. структуру файла ИТ-архитектура.xlsx).
      - Проектирование и внедрение отказоустойчивой сетевой инфраструктуры (внутри нового здания, между филиалами, DMZ, SCADA, Wi-Fi, IP-телефония).
      - Проектирование и оснащение серверной (ЦОД) в новом здании с учетом требований к энергоснабжению, охлаждению, ИБ.
      - Подбор и закупка необходимого серверного и сетевого оборудования, СХД, систем ИБ.
      - Разработка и внедрение комплексной системы информационной безопасности.
      - Обеспечение интеграции ключевых систем предприятия (ERP 1С, CRM Bitrix24/ ELMA365, BI QLIK, облачные сервисы, СУБД, производственные системы).
      - Настройка процессов управления ИТ-услугами (ITSM) и поддержки.
      - Обеспечение резервного копирования данных и разработка плана восстановления (BC/DR).
      - Тестирование и ввод в эксплуатацию новой ИТ-инфраструктуры.
   2.3. Установление измеримых критериев успеха (KPIs):
      - Снижение времени простоя критических ИТ-систем (например, менее 1 часа в месяц).
      - Достижение заявленной производительности сетевого канала между филиалами и головным офисом (например, >95% от заявленной пропускной способности).
      - Успешное прохождение тестов отказоустойчивости кластеров и систем хранения.
      - Соответствие параметров охлаждения и энергоснабжения серверной проектным значениям.
      - Положительная оценка удовлетворенности пользователей по результатам UAT.
      - Успешное прохождение тестов информационной безопасности.
      - Соблюдение сроков и бюджета проекта (отклонение < X%).
      - Полное выполнение всех пунктов плана миграции/переезда без потерь данных.
3. Сбор и анализ высокоуровневых требований:
   3.1. Какие типы производственных систем и автоматизированных комплексов будут использоваться:

- Идентификация используемых или планируемых к внедрению АСУ ТП, MES, SCADA и других промышленных систем.
- Определение критичности этих систем для бизнеса и требований к их доступности.
- Уточнение специфических требований к ИТ-инфраструктуре для поддержки данных систем (например, низкие задержки, изоляция).

3.2. Анализ объема данных, которые будут генерироваться:
- Оценка текущего объема структурированных и неструктурированных данных.
- Прогноз роста объемов данных в среднесрочной и долгосрочной перспективе.
- Определение типов данных (транзакционные, аналитические, файлы, мультимедиа) и требований к их хранению и обработке.

3.3. Оценка производительности сети:
- Анализ текущих требований к пропускной способности внутри офисов и между филиалами.
- Определение требований к задержкам и jitter для критичных приложений (голос, видео, промышленные системы).
- Идентификация пиковых нагрузок и необходимой резервной пропускной способности.

3.4. Интеграция с какими системами понадобится (ERP, CRM и т. д.):
- Составление перечня существующих и планируемых к внедрению ИТ-систем (ERP 1С, CRM Bitrix24/ELMA365, BI QLIK, облачные сервисы и др.).
- Определение направлений и требований к интеграции между этими системами и другими компонентами ИТ-ландшафта.
- Уточнение используемых протоколов и интерфейсов интеграции.

3.5. Система Авторизации:
- Определение требований к единой системе идентификации и аутентификации пользователей.
- Выбор технологии (например, Microsoft Active Directory, LDAP, SSO решения).
- Уточнение требований к управлению привилегиями и доступом (PAM, RBAC).

3.6. Анализ рисков: Идентификация потенциальных рисков проекта (технические, организационные, финансовые, сроки) и разработка стратегии их минимизации.

3.7. Управление заинтересованными сторонами (Stakeholder Management): Определение ключевых лиц, принимающих решения, и пользователей; планирование коммуникаций с ними.

3.8. Оценка текущих ИТ-активов (Inventory): Если есть существующая инфраструктура, важно понять, что можно использовать повторно, а что подлежит замене/модернизации.

3.9. Определение метрик успеха (KPIs): Конкретные измеримые показатели, по которым будет оцениваться успешность реализации архитектуры (время отклика системы, уровень доступности, время восстановления после сбоя и т.д.).

4. Формирование проектной команды:

4.1. Представители заказчика (внутренние сотрудники):
- Руководитель ИТ-подразделения или CIO предприятия.
- Архитектор ИТ/Ведущий специалист ИТ.
- Специалисты по сетям, системному администрированию, информационной безопасности (в зависимости от структуры ИТ-отдела заказчика).
- Представители бизнес-подразделений (производство, бухгалтерия, отдел продаж), ключевые пользователи будущих систем.
- Специалист по закупкам/контрактному управлению со стороны заказчика (если требуется).

4.2. Генеральный подрядчик (если проект выполняется силами одного основного исполнителя):
- Руководитель проекта от Генподрядчика.
- Ведущий ИТ-архитектор / Консультант от Генподрядчика.
- Специалисты по сетям, серверам, ИБ, интеграции, ПО от Генподрядчика.

4.3. Субподрядчики и поставщики (если привлекаются специализированные компании):

- Компании, специализирующиеся на проектировании и строительстве ЦОД/серверных (инженерные системы, отделка).
- Поставщики сетевого оборудования, серверов, СХД, ИБП, систем ИБ.
- Специализированные компании по интеграции конкретных решений (например, SCADA, ERP, CRM, BI).
- Консультанты по отдельным направлениям (например, ИБ, ITSM).

5. Создание плана проекта (сроки, бюджет, риски, коммуникации):

5.1. Определение сроков проекта:

- Разработка графика выполнения работ (диаграмма Ганта) с детализацией по этапам и ключевым вехам.
- Установление взаимосвязей между задачами и определение критического пути.
- Согласование сроков с ключевыми заинтересованными сторонами.
- Определение сроков для каждой фазы проекта (Инициация, Анализ и Проектирование, Подготовка, Внедрение, Тестирование, Go-Live/Поддержка).
- Планирование сроков поставок оборудования и лицензий ПО.
- Резервы времени на непредвиденные обстоятельства.

5.2. Формирование бюджета проекта:

- Составление сметы по статьям расходов: оборудование, программное обеспечение, работы подрядчиков (проектирование, монтаж, интеграция, внутренние ресурсы, обучение, тестирование.
- Учет стоимости лицензий, гарантийного и постгарантийного обслуживания.
- Резерв на непредвиденные расходы.
- Установление порядка контроля и отчетности по бюджету.
- Согласование бюджета с финансовыми службами заказчика.

5.3. Идентификация и анализ рисков:

- Проведение детального анализа потенциальных рисков: технические (несовместимость, производительность), организационные (изменения в команде, приоритетах), финансовые (превышение бюджета), временные (срыв сроков поставок, задержки строительства серверной).
- Оценка вероятности наступления и потенциального влияния каждого риска.
- Разработка плана реагирования на риски: избежать, принять, смягчить, передать (например, через договоры с подрядчиками).
- Назначение владельцев рисков.
- Планирование регулярного мониторинга и обновления реестра рисков в ходе проекта.

5.4. Планирование коммуникаций:

- Определение ключевых заинтересованных сторон и их информационных потребностей.
- Установление периодичности и форматов отчетности (еженедельные/ежемесячные отчеты, встречи, дашборды).
- Выбор каналов коммуникации (почта, видеоконференции, корпоративные порталы).
- Определение ответственных за предоставление информации.
- Планирование встреч по управлению проектом, технических обзоров, встреч с комитетом по ИТ или руководством.
- Создание плана информирования пользователей о ходе проекта и предстоящих изменениях.

6. Утверждение общего подхода к архитектуре:

6.1. Формулирование принципов проектирования ИТ-архитектуры:

- Единая, масштабируемая и отказоустойчивая архитектура для всего предприятия, включая головной офис и филиалы.
- Использование стандартизированных, проверенных решений и технологий, обеспечивающих совместимость и упрощающих поддержку.

- Модульность и гибкость архитектуры, позволяющие адаптироваться к изменяющимся бизнес-потребностям.
- Приоритет информационной безопасности на всех уровнях (сети, приложения, данные, физическая безопасность).
- Централизованное управление ИТ при обеспечении необходимой автономии филиалов.
- Оптимизация совокупной стоимости владения (TCO) с учетом затрат на закупку, внедрение, эксплуатацию и развитие.
- Использование лучших отраслевых практик (например, ITIL для ITSM, ISO 27001 для ИБ).

6.2. Определение ключевых архитектурных решений:
- Модель размещения ИТ-ресурсов: централизованная (основной ЦОД) с возможными локальными узлами в ключевых филиалах.
- Стратегия виртуализации серверов и инфраструктуры (VMware, Hyper-V, и т.д.).
- Подход к построению сетевой инфраструктуры: иерархическая модель (ядро, распределение, доступ), использование SDN.
- Стратегия хранения данных: тип СХД, политики резервного копирования, архивирования, репликации.
- Подход к интеграции систем: использование ESB, API, стандартов интеграции.
- Архитектура систем информационной безопасности: многоуровневая защита, Zero Trust (если применимо).
- Стратегия использования облачных сервисов (SaaS, IaaS, PaaS) vs. on-premise решений.

6.3. Согласование концепции архитектуры с заинтересованными сторонами:
- Проведение презентации предложенной архитектурной концепции для ключевых лиц заказчика (IT-директор, бизнес-заказчики, финансовый директор).
- Обсуждение компромиссов между различными требованиями (производительность, безопасность, стоимость, сроки).
- Получение формального одобрения выбранного архитектурного подхода от комитета по ИТ или руководства предприятия.
- Фиксация утвержденного подхода в документе "Архитектурный принцип" или аналогичном.

6.4. Определение ограничений и допущений:
- Четкое обозначение факторов, которые ограничивают выбор решений (бюджет, существующие контракты, нормативные требования).
- Формулировка допущений, на которых базируется архитектура (например, стабильность требований к объему данных в течение ближайших N лет).
- Установление критериев, при изменении которых может потребоваться пересмотр архитектурного подхода.

Результат этапа 1:

1. Устав проекта:
1.1. Официальное утверждение проекта руководством заказчика.
1.2. Четкое определение целей и задач проекта.
1.3. Назначение ответственных лиц (спонсора, менеджера проекта).
1.4. Определение границ проекта (что входит, что не входит).
1.5. Установление общего бюджета и сроков проекта.
1.6. Определение ключевых заинтересованных сторон.

2. Предварительный план проекта:
2.1. Общий график выполнения работ (календарный план-график).
2.2. Предварительная оценка бюджета по основным категориям (оборудование, ПО, работы).

2.3. Идентификация основных рисков проекта.
2.4. План коммуникаций с ключевыми участниками.
2.5. Перечень основных этапов и ключевых контрольных точек (milestones).
2.6. Предварительное распределение ресурсов.

3. Созданный раздел "Оценка и планирование":
3.1. Заполненная информация о типах используемых производственных систем и автоматизированных комплексов.
3.2. Данные по анализу объема генерируемых данных.
3.3. Результаты оценки требований к производительности сети.
3.4. Перечень систем, требующих интеграции (ERP, CRM и др.).
3.5. Определенные подходы и требования к системе авторизации.
3.6. Начальный список идентифицированных рисков.
3.7. Карта заинтересованных сторон проекта.
3.8. Инвентаризация существующих ИТ-активов (при наличии).
3.9. Набор предварительных KPIs проекта.

Этап 2: Анализ и Проектирование
(AS-IS И TO-BE, КАК ЕСТЬ -> КАК БУДЕТ)

Цель: Глубоко понять текущее состояние ИТ (если есть) и спроектировать целевую архитектуру.

Деятельность:

1. Анализ текущего состояния (As-Is - Как есть):
   1.1. Аудит существующей ИТ-инфраструктуры:
      - Исследование и инвентаризация текущих сетевых устройств, серверов, систем хранения данных (СХД), программного обеспечения, средств информационной безопасности (ИБ).
      - Оценка состояния, производительности и ресурсов каждого компонента.
      - Выявление узких мест, ограничений и потенциальных точек отказа.
   1.2. Картирование бизнес-процессов и их зависимости от ИТ:
      - Идентификация ключевых бизнес-процессов предприятия.
      - Определение ИТ-систем и инфраструктурных компонентов, критически важных для функционирования каждого процесса.
      - Создание карты взаимосвязей бизнес-процессов и ИТ-активов.
   1.3. Анализ требований по производительности, отказоустойчивости, безопасности:
      - Сбор и анализ требований к доступности, производительности и безопасности от бизнес-пользователей и ИТ-персонала.
      - Сопоставление текущего уровня соответствия этим требованиям.
      - Определение пробелов между текущим состоянием и ожиданиями.

2. Проектирование целевой архитектуры (To-Be - Как будет):
   2.1. Завершение раздела "Оценка и планирование":
      - Финализация и детализация всех пунктов, начатых в Этапе 1, на основе данных анализа As-Is.
   2.2. Разработка детальной топологии сетей:
      2.2.1. Каналы связи:
         - Выбор типов каналов связи (выделенные линии, MPLS, VPN) между головным офисом, филиалами и внешними ресурсами.
         - Определение требуемой пропускной способности для каждого канала.
         - Выбор поставщиков услуг связи.
      2.2.2. Каналы доступов и маршрутизации (ospf, bgp, vpn):
         - Проектирование протоколов внутренней (OSPF) и внешней (BGP) маршрутизации.
         - Проектирование VPN-подключений для удаленных пользователей и филиалов.
         - Определение схемы адресации и зон ответственности.
      2.2.3. Управляемые сети SDN, Автоматизация и мониторинг:
         - Оценка необходимости и проектирование сегментов Software-Defined Networking.
         - Планирование автоматизации сетевых процессов.
         - Выбор инструментов для мониторинга сетевой инфраструктуры.
      2.2.4. Подбор сетевого оборудования и ПО:
         - Формирование спецификаций для коммутаторов, маршрутизаторов, межсетевых экранов и другого сетевого оборудования.
         - Выбор сетевого ПО (NOC, системы управления).
      2.2.5. Демилитаризованная зона (DMZ):

- Проектирование архитектуры DMZ для размещения серверов, доступных из интернета.
- Определение правил фильтрации трафика между зонами.

2.2.6. Зона SCADA:
- Проектирование изолированного сегмента сети для подключения систем диспетчеризации и управления производственными процессами.
- Определение мер безопасности для зоны SCADA.

2.2.7. Система привилегированного доступа (PAM):
- Проектирование системы управления привилегированным доступом к критическим ИТ-ресурсам.

2.2.8. Подключение мобильных и удалённых активов:
- Проектирование безопасных каналов доступа для мобильных сотрудников и удаленных офисов.

2.2.9. Тестовая среда:
- Проектирование изолированной тестовой среды, зеркальной основной архитектуре.

2.2.10. Проект WIFI:
- Проектирование беспроводной сети для офисов, определение зон покрытия, требований безопасности.

2.2.11. IP-телефония:
- Проектирование инфраструктуры IP-телефонии, включая АТС, шлюзы, терминалы, требования к QoS.

2.3. Проектирование аппаратного обеспечения:

2.3.1. Серверы:
- Подбор серверов под конкретные роли (приложения, базы данных, виртуализация) с учетом требований к производительности и отказоустойчивости.

2.3.2. Периферийные устройства:
- Определение необходимых периферийных устройств (принтеры, сканеры и т.д.) и способов их подключения/управления.

2.3.3. Промышленное сетевое оборудование:
- Подбор специализированного сетевого оборудования для подключения к производственным системам (если требуется).

2.3.4. Системы хранения данных (СХД):
- Выбор типа СХД (DAS, NAS, SAN), определение требований к объему, производительности, надежности, резервному копированию.

2.3.5. Шлюзы и сетевые экраны:
- Подбор и позиционирование шлюзов и межсетевых экранов для обеспечения безопасности и маршрутизации.

2.4. Разработка проекта информационной безопасности:

2.4.1. Проект антивирусной защиты:
- Выбор комплексного решения для защиты от вредоносного ПО на серверах и рабочих станциях.

2.4.2. Проект видеонаблюдения:
- Проектирование системы видеонаблюдения для физической защиты объектов ИТ (серверные, ЦОД).

2.4.3. Проект СКУД:
- Проектирование системы контроля и управления доступом в помещения ИТ.

2.4.4. Проект положения и доступов:
- Разработка политик и регламентов по управлению доступом к ИТ-ресурсам.

2.4.5. Проект межсетевых экранов:
- Детализация правил фильтрации трафика на всех межсетевых экранах.

2.4.6. Проект организации VPN доступов:

- Детализация архитектуры и политик безопасности для VPN-подключений.

2.4.7. Проект резервного копирования:

- Проектирование стратегии резервного копирования.

2.5. Проектирование серверной и кластерной инфраструктуры :

2.5.1. Проектирование серверной:

- Детальное проектирование ЦОД/серверной комнаты, включая требования к энергоснабжению, охлаждению, пожарной безопасности, физической безопасности.

2.5.2. Проект СХД:

- Детализация проекта СХД.

2.5.3. Проект кластерной инфраструктуры:

- Проектирование отказоустойчивых кластеров для критически важных сервисов.

2.5.4. ИБП:

- Подбор и проектирование системы бесперебойного питания для ИТ-оборудования.

2.6. Проектирование Интеграции систем:

2.6.1. Проект по базам данных:

- Определение архитектуры СУБД, требований к производительности, отказоустойчивости, резервному копированию.

2.6.2. ERP (1С):

- Проектирование архитектуры и интеграции ERP-системы 1С.

2.6.3. CRM (Bitrix24, ELMA365):

- Проектирование архитектуры и интеграции CRM-систем.

2.6.4. CLOUD, облачные решения:

- Определение стратегии использования облачных сервисов, модели развертывания, интеграции с внутренними системами.

2.6.5. BI (QLIK):

- Проектирование архитектуры и интеграции BI-решения QLIK.

2.7. Проектирование ITSM процессов:

2.7.1. Кто будет заниматься поддержкой и управлением новыми системами?:

- Определение ролей и ответственности в рамках процессов управления ИТ-услугами.

2.7.2. Организация работы отделов:

- Проектирование взаимодействия ИТ-отделов между собой и с бизнес-подразделениями в рамках ITSM.

2.8. Проектирование Почты:

- Проектирование архитектуры корпоративной почтовой системы (внутренний сервер или облачное решение), обеспечение безопасности и резервного копирования.

2.9. Проектирование Хранения и учета документации (файловые сервера):

- Проектирование файловых ресурсов, включая структуру каталогов, права доступа, резервное копирование, возможно, внедрение DMS.

2.10. Проектирование Организации работы Бухгалтерии:

- Проектирование ИТ-решений, специфичных для задач бухгалтерского учета и отчетности.

2.11. Проектирование Интеграции производственных систем:

- Проектирование архитектуры и способов интеграции производственных систем (SCADA, MES) с ИТ-ландшафтом предприятия.

2.12. Проектирование процессов резервного копирования и восстановления (BC/DR):
- Подробный план того, что, как часто и куда резервируется, стратегии резервного копирования (Full/Incremental/Differential), политики хранения, план восстановления и тестирования восстановления (RTO/RPO для критичных систем).
- Планирование Disaster Recovery (DR) плана: действия на случай крупной аварии, площадка для аварийного восстановления, процедуры переключения.

2.13. Проектирование мониторинга и управления:
- Выбор инструментов и определение метрик для мониторинга состояния инфраструктуры (серверов, сетей, СХД, приложений). Определение порогов срабатывания и процессов реагирования. Проектирование системы логирования и аудита.

2.14. Проектирование управления жизненным циклом ИТ-активов:
- Как будет вестись учет оборудования и ПО, процессы закупки, ввода в эксплуатацию, обновления, вывода из эксплуатации.

2.15. Проектирование управления изменениями (Change Management):
- Процесс, по которому будут вноситься изменения в ИТ-инфраструктуру после ввода в эксплуатацию.

Результат Этап 2:

1. Документы ИТ-архитектуры по каждому из 12 разделов:
1.1. Заполненный и детализированный раздел "Оценка и планирование", содержащий окончательные данные по используемым системам, объемам данных, сетевым требованиям, интеграциям и авторизации.
1.2. Детализированный проект "Топология сетей", включающий схемы, спецификации оборудования, планы адресации, маршрутизации и безопасности.
1.3. Детализированный "Проект аппаратного обеспечения" со списками и характеристиками всего необходимого серверного, сетевого и периферийного оборудования.
1.4. Детализированный "Проект ИБ", описывающий меры безопасности по всем направлениям (антивирус, видеонаблюдение, СКУД, ИБП, резервное копирование и т.д.).
1.5. Детализированный раздел "ITSM (Service Management)", определяющий процессы поддержки, роли и организацию работы ИТ-отдела.
1.6. Детализированное "Проектирование серверной", включая проекты СХД, кластеров и ИБП.
1.7. Детализированный план "Внедрение и конфигурирование систем", описывающий этапы установки, настройки и тестирования.
1.8. Детализированный проект "Интеграции систем", содержащий схемы и методы интеграции ERP, CRM, BI, облачных решений и СУБД.
1.9. Проект "Организации работы Бухгалтерии".
1.10. Проект "Системы хранения и учета документации (файловые сервера)".
1.11. Проект "Интеграции производственных систем".
1.12. Проект "Почтовых ресурсов".

2. Технические спецификации оборудования и ПО:
2.1. Спецификации сетевого оборудования (маршрутизаторы, коммутаторы, межсетевые экраны, точки доступа и т.д.) с точными моделями, количеством и характеристиками.
2.2. Спецификации серверного оборудования (серверы, СХД) с указанием конфигураций (ЦП, память, накопители).

2.3. Спецификации периферийного и промышленного оборудования.
2.4. Перечень необходимого программного обеспечения (операционные системы, СУБД, приложения, лицензии, антивирусы, системы мониторинга, ИБ и т.д.) с версиями и количеством лицензий.

3. Схемы сетевой и системной архитектуры:
3.1. Архитектурные схемы сетевой инфраструктуры предприятия (топология, зоны, маршрутизация, DMZ, SCADA).
3.2. Схемы размещения сетевого оборудования.
3.3. Схемы размещения серверного оборудования и СХД.
3.4. Схемы интеграции ИТ-систем (ERP, CRM, BI, облачные сервисы, производственные системы).
3.5. Схемы развертывания систем безопасности (ИБП, СКУД, видеонаблюдение).
3.6. Схема тестовой среды.

4. План перехода (Transition Plan) от As-Is к To-Be (если применимо):
4.1. Описание текущего состояния ИТ (As-Is) на основе проведенного анализа.
4.2. Последовательность ключевых этапов перехода от текущего к целевому состоянию.
4.3. План миграции данных (если требуется).
4.4. План переключения критических сервисов.
4.5. Риски, связанные с переходом, и меры по их минимизации.
4.6. Необходимые ресурсы (человеческие, технические, временные) для выполнения перехода.

Этап 3: Подготовка к Внедрению
(ЗАКУПКИ, ПОДГОТОВКА)

Цель: Подготовить все необходимое для реализации спроектированной архитектуры.

Деятельность:

1. Формирование технических заданий и спецификаций для закупок:
   1.1. Сбор и консолидация всех технических спецификаций, разработанных на Этапе 2 (оборудование, ПО, услуги).
   1.2. Подготовка технических заданий (ТЗ) для каждого типа закупки (оборудование, лицензии ПО, услуги по монтажу, интеграции, аутсорсинг ИБ и т.д.).
   1.3. Уточнение требований к поставщикам (сертификаты, опыт, финансовая стабильность, сервисная поддержка).
   1.4. Подготовка технической документации для включения в конкурсные материалы или запросы коммерческих предложений (RFP/RFQ).

2. Проведение тендеров или согласование условий с поставщиками:
   2.1. Определение процедуры закупки (тендер, запрос котировок, переговоры с единственным поставщиком) для каждой позиции.
   2.2. Публикация конкурсной документации (при необходимости) и прием заявок/предложений.
   2.3. Оценка коммерческих и технических предложений поставщиков согласно заранее определенным критериям.
   2.4. Проведение презентаций и технических обсуждений с финалистами.
   2.5. Выбор оптимального поставщика для каждой категории закупок.

3. Заключение контрактов:
   3.1. Подготовка и согласование договоров с выбранными поставщиками.
   3.2. Включение в договоры ключевых условий: сроки поставки и выполнения работ, гарантии, уровень сервиса (SLA), условия оплаты, ответственность сторон.
   3.3. Юридическая экспертиза договоров.
   3.4. Формальное подписание контрактов с поставщиками и подрядчиками.

4. Подготовка площадки (строительство/ремонт серверной, подготовка помещений под оборудование):
   4.1. Координация строительно-монтажных работ по подготовке помещений под ЦОД/серверную и другие ИТ-зоны.
   4.2. Контроль выполнения инженерных систем (электричество, вентиляция, пожарная безопасность, СКС) в соответствии с проектом.
   4.3. Подготовка помещений для размещения конечного пользовательского оборудования (офисы, рабочие места).
   4.4. Приемка готовых помещений и инженерных коммуникаций.

5. Подготовка команды к внедрению (обучение, настройка процессов):
   5.1. Определение требуемых навыков у внутренней ИТ-команды для эксплуатации новой архитектуры.
   5.2. Планирование и организация обучения персонала работе с новыми системами, оборудованием, инструментами мониторинга и управления.
   5.3. Настройка внутренних процессов ИТ-отдела в соответствии с новой архитектурой и ITSM.
   5.4. Подготовка (или привлечение) специалистов-подрядчиков, если требуется дополнительная экспертиза для внедрения.

6. Планирование миграции данных:
   6.1. Детальное планирование процесса переноса существующих данных (при замене/обновлении систем).
   6.2. Определение объемов и типов данных для миграции.
   6.3. Разработка процедур очистки, преобразования (трансформации) и валидации данных перед и после переноса.
   6.4. Планирование окон миграции с минимальным влиянием на бизнес.
   6.5. Подготовка плана отката на случай сбоев миграции.

7. Подготовка документации:
   7.1. Создание или обновление эксплуатационной документации для всех новых компонентов ИТ-инфраструктуры.
   7.2. Разработка или актуализация руководств администратора по настройке и управлению системами.
   7.3. Подготовка или обновление политик и регламентов ИТ (безопасность, резервное копирование, управление изменениями и т.д.).
   7.4. Систематизация всей проектной документации для передачи в эксплуатацию.

8. Планирование коммуникаций:
   8.1. Разработка плана информирования пользователей и заинтересованных сторон о ходе проекта, предстоящих изменениях и их влиянии.
   8.2. Создание информационных материалов (новости, инструкции, уведомления).
   8.3. Определение каналов коммуникации (электронная почта, корпоративный портал, собрания).
   8.4. Информирование о графике работ, возможных простоях или ограничениях в работе ИТ-сервисов.

9. (Параллельно) Начало подготовки тестовой среды:
   9.1. Закупка/выделение оборудования для тестовой среды (может быть частью общей закупки).
   9.2. Подготовка инфраструктуры тестовой среды (монтаж, сетевые настройки).
   9.3. Начальная настройка и развертывание базовых сервисов в тестовой среде.
   9.4. Подготовка к проведению тестирования (функциональное, интеграционное, нагрузочное).

Результат Этап 3:

1. Закупленное оборудование и лицензии ПО:
   1.1. Всё необходимое серверное, сетевое и периферийное оборудование, приобретенное в соответствии со спецификациями.
   1.2. Все необходимые лицензии на программное обеспечение, включая операционные системы, прикладные программы, антивирусы, СУБД и т.д.
   1.3. Подтверждение получения оборудования и лицензий, проверка комплектности.

2. Подписанные контракты:
   2.1. Заключенные и подписанные договоры с поставщиками оборудования и лицензий.
   2.2. Заключенные и подписанные договоры с подрядчиками на выполнение работ (монтаж, интеграция, консалтинг и т.д.).
   2.3. Договоры на гарантийное и постгарантийное обслуживание ключевых компонентов ИТ-инфраструктуры.

3. Готовая инфраструктурная база (помещения, коммуникации):

3.1. Приемка и готовность помещений под ЦОД/серверную, включая все инженерные системы (электричество, охлаждение, пожарная безопасность, СКС).
3.2. Готовность других ИТ-зон и пользовательских помещений.
3.3. Установленные и протестированные базовые коммуникации (электропитание, сетевые кабели, розетки).

4. Подготовленная команда:
4.1. Внутренняя ИТ-команда, прошедшая необходимое обучение для работы с новой архитектурой.
4.2. Настроенные процессы и процедуры внутри ИТ-отдела.
4.3. Привлеченные специалисты-подрядчики (при необходимости).
4.4. Готовность команды к выполнению задач Этапа 4 "Внедрение и Конфигурирование".

Этап 4: Внедрение и Конфигурирование
(РЕАЛИЗАЦИЯ TO-BE)

Цель: Физически реализовать спроектированную ИТ-архитектуру.

Деятельность:

1. Монтаж и установка сетевого оборудования, серверов, СХД, ИБП:
   1.1. Организация и проведение работ по установке серверного оборудования в ЦОД/серверной.
   1.2. Монтаж сетевого оборудования (коммутаторы, маршрутизаторы, межсетевые экраны) в соответствии со схемами топологии.
   1.3. Установка и подключение систем хранения данных (СХД).
   1.4. Монтаж и подключение источников бесперебойного питания (ИБП).
   1.5. Установка и подключение периферийных устройств.
   1.6. Проверка правильности физической установки, подключения к электропитанию и кабельной инфраструктуре.
   1.7. Первичная проверка работоспособности установленного оборудования.

2. Настройка сетевой инфраструктуры (маршрутизация, коммутация, ИБ, VPN):
   2.1. Конфигурирование коммутаторов (VLAN, STP, QoS, безопасность портов).
   2.2. Настройка маршрутизаторов (статическая/динамическая маршрутизация OSPF/BGP, NAT, ACL).
   2.3. Конфигурирование межсетевых экранов (правила фильтрации трафика, зоны, NAT, VPN-туннели).
   2.4. Настройка VPN-подключений для филиалов и удаленных пользователей.
   2.5. Настройка параметров безопасности сети.
   2.6. Проведение тестов сетевой связности и проверка политик безопасности.

3. Установка и настройка операционных систем, СУБД, приложений, СХД:
   3.1. Установка операционных систем на серверы и рабочие станции в соответствии с проектными спецификациями.
   3.2. Базовая настройка ОС (пользователи, политики безопасности, обновления).
   3.3. Установка и настройка серверов баз данных (СУБД).
   3.4. Установка и первоначальная настройка серверных приложений (ERP, CRM, BI, почта и др.).
   3.5. Настройка систем хранения данных (СХД) - создание пулов, LUN'ов, подключение к серверам.
   3.6. Установка клиентского программного обеспечения на рабочие станции пользователей.

4. Интеграция систем (настройка API, соединений, синхронизации данных):
   4.1. Настройка API и интерфейсов для взаимодействия между ключевыми ИТ-системами (ERP, CRM, BI, облачные сервисы и др.).
   4.2. Конфигурирование соединений между системами (базы данных, файловые шары, веб-сервисы).
   4.3. Настройка механизмов синхронизации данных между интегрируемыми системами.
   4.4. Тестирование корректности обмена данными между системами.

5. Настройка систем ИБ (антивирусы, межсетевые экраны, PAM):
   5.1. Развертывание и настройка антивирусного ПО на серверах и рабочих станциях.
   5.2. Финальная настройка правил межсетевых экранов.

5.3. Внедрение и настройка системы привилегированного доступа (PAM).
5.4. Настройка других компонентов ИБ (СКУД для серверной, видеонаблюдение).
5.5. Проверка и тестирование эффективности мер информационной безопасности.

6. Настройка систем мониторинга:
6.1. Установка и настройка платформы мониторинга ИТ-инфраструктуры.
6.2. Добавление в мониторинг серверов, сетевого оборудования, СХД, приложений.
6.3. Настройка сбора метрик (CPU, память, диск, сеть) и логов.
6.4. Определение порогов срабатывания алертов и настройка уведомлений.
6.5. Настройка дашбордов для визуализации состояния ИТ.

7. Настройка ITSM процессов и инструментов:
7.1. Развертывание (если требуется) и настройка инструментов управления ИТ-услугами (Helpdesk, CMDB, система управления инцидентами/проблемами/изменениями).
7.2. Настройка ролей и прав доступа в ITSM-системе.
7.3. Внедрение и адаптация процессов ITSM (управление инцидентами, запросами, проблемами, изменениями, конфигурациями) в соответствии с проектом.
7.4. Обучение персонала работе с ITSM-процессами и инструментами.

8. Настройка почты:
8.1. Финальная настройка серверов почтовой системы или облачного почтового сервиса.
8.2. Создание учетных записей пользователей, групп рассылки.
8.3. Настройка политик безопасности электронной почты (фильтрация спама, антивирус).
8.4. Настройка клиентов электронной почты у пользователей.

9. Настройка файловых ресурсов:
9.1. Настройка файловых серверов или NAS/SAN.
9.2. Создание структуры сетевых папок и настройка прав доступа согласно политикам.
9.3. Настройка резервного копирования файловых ресурсов.
9.4. Предоставление доступа пользователям к файловым ресурсам.

10. Настройка IP-телефонии и Wi-Fi:
10.1. Настройка сервера IP-телефонии (АТС) и шлюзов.
10.2. Конфигурирование IP-телефонов, настройка номеров и маршрутов.
10.3. Настройка параметров QoS в сети для обеспечения качества голосовой связи.
10.4. Настройка контроллеров беспроводной сети и точек доступа Wi-Fi.
10.5. Настройка ssid, безопасности (шифрование, аутентификация) и зон покрытия Wi-Fi.
10.6. Тестирование работы IP-телефонии и беспроводной сети.

11. Первоначальное наполнение данными (если требуется):
11.1. Загрузка или миграция начальных данных в новые системы (если не проводилась на этапе 3).
11.2. Валидация корректности загруженных данных.
11.3. Настройка пользовательских профилей и начальных настроек в приложениях.

12. Настройка резервного копирования:
12.1. Установка и настройка программного обеспечения для резервного копирования.
12.2. Настройка заданий резервного копирования для всех критичных данных и систем.

12.3. Настройка политик хранения резервных копий.
12.4. Проверка возможности восстановления данных из резервных копий.

13. Управление конфигурацией:
13.1. Идентификация и регистрация всех конфигурационных единиц (CI) - оборудования, ПО, сервисов - в CMDB.
13.2. Заполнение атрибутов CI (модель, серийный номер, IP-адрес, место установки, статус и т.д.).
13.3. Установление взаимосвязей между CI.
13.4. Поддержание актуальности информации в CMDB в процессе внедрения.

14. Контроль качества (QA):
14.1. Проведение промежуточных проверок выполненных работ на соответствие проектной документации и техническим спецификациям.
14.2. Аудит настроек оборудования и ПО на соответствие стандартам и политикам безопасности.
14.3. Документирование выявленных несоответствий и контроль их устранения.
14.4. Подготовка отчетов о результатах контроля качества.

Результат Этап 4:

1. Функционирующая ИТ-инфраструктура в соответствии с проектом:
1.1. Установленное, сконфигурированное и протестированное серверное оборудование.
1.2. Настроенная и функционирующая сетевая инфраструктура (коммутация, маршрутизация, ИБ, VPN).
1.3. Установленные и настроенные операционные системы, СУБД и приложения.
1.4. Работающие интеграции между ключевыми ИТ-системами.
1.5. Внедренные и функционирующие системы информационной безопасности.
1.6. Настроенная и работающая система мониторинга ИТ-ландшафта.
1.7. Настроенные и функционирующие ITSM-процессы и инструменты.
1.8. Настроенная корпоративная почтовая система.
1.9. Доступные и настроенные файловые ресурсы.
1.10. Работающая IP-телефония и беспроводная сеть Wi-Fi.
1.11. Настроенная система резервного копирования.
1.12. Заполненная и актуальная CMDB.

Этап 5: Тестирование и Валидация

Цель: Убедиться, что внедренная архитектура соответствует требованиям.

Деятельность:

1. Проведение различных видов тестирования:
   1.1. Функциональное тестирование:
   - Проверка корректности работы каждого компонента ИТ-инфраструктуры (серверы, сети, СХД, приложения) в соответствии с проектной документацией.
   - Верификация настроек операционных систем, СУБД, систем мониторинга, ИБ.
   1.2. Нагрузочное тестирование (Performance Testing):
   - Проверка производительности системы под ожидаемой и пиковой нагрузкой.
   - Оценка времени отклика ключевых сервисов и приложений.
   - Проверка пропускной способности сетевых каналов.
   - Определение максимальной нагрузки, которую может выдержать инфраструктура.
   1.3. Тестирование информационной безопасности (Security Testing):
   - Проверка корректности работы средств ИБ (антивирусы, межсетевые экраны, PAM).
   - Тестирование на проникновение (Penetration Testing) для выявления уязвимостей.
   - Проверка соответствия политикам и стандартам ИБ предприятия.
   - Аудит прав доступа пользователей и администраторов.
   1.4. Тестирование восстановления из резервных копий:
   - Проверка возможности и полноты восстановления данных из резервных копий.
   - Измерение времени восстановления (RTO) и точки восстановления (RPO) для критичных систем.
   - Валидация целостности восстановленных данных.

2. Тестирование интеграций между системами:
   2.1. Проверка корректности обмена данными между интегрированными системами (ERP, CRM, BI, облачные сервисы и др.).
   2.2. Тестирование синхронизации данных в различных сценариях.
   2.3. Проверка обработки ошибок и исключительных ситуаций в интеграционных потоках.
   2.4. Верификация безопасности передачи данных между системами.

3. Тестирование аварийного восстановления (Disaster Recovery Testing):
   3.1. Проведение симуляции аварийной ситуации (отключение питания, выход из строя канала связи и т.д.).
   3.2. Проверка работоспособности плана аварийного восстановления (DR Plan), разработанного на Этапе 2 (п. 2.12).
   3.3. Тестирование переключения на резервную площадку (hot/warm site) или восстановление критичных сервисов.
   3.4. Измерение времени переключения и восстановления критичных бизнес-функций.

4. User Acceptance Testing (UAT):
   4.1. Организация и проведение тестирования системы конечными пользователями.
   4.2. Предоставление пользователям тестовой среды или ограниченного доступа к новой системе.
   4.3. Проверка соответствия системы бизнес-требованиям и ожиданиям пользователей.
   4.4. Сбор обратной связи и замечаний от пользователей.

4.5. Формализация критериев приемки системы пользователями.

5. Обучение пользователей (если требует архитектура):
5.1. Проведение тренингов и обучающих сессий для конечных пользователей по работе с новыми или обновленными ИТ-системами.
5.2. Предоставление обучающих материалов (инструкции, видео, справочники).
5.3. Поддержка пользователей на этапе тестирования и в ходе UAT.

6. Корректировка конфигураций по результатам тестирования:
6.1. Анализ результатов всех видов тестирования.
6.2. Идентификация и документирование выявленных замечаний, ошибок, несоответствий.
6.3. Приоритизация замечаний и определение плана их устранения.
6.4. Внесение необходимых изменений в конфигурацию оборудования, ПО, политик безопасности, интеграций и т.д.
6.5. Повторное тестирование исправленных элементов (регрессионное тестирование).

Результат Этап 5:

1. Протоколы тестирования:
1.1. Протоколы функционального тестирования компонентов ИТ-инфраструктуры.
1.2. Отчеты по результатам нагрузочного тестирования (Performance Testing Reports).
1.3. Отчеты по результатам тестирования информационной безопасности (Security Test Reports).
1.4. Протоколы тестирования восстановления из резервных копий.
1.5. Протоколы тестирования интеграций между системами.
1.6. Отчеты по результатам тестирования аварийного восстановления (DR Test Reports).
1.7. Протоколы User Acceptance Testing (UAT Reports) с подписями ответственных лиц.

2. Устраненные замечания:
2.1. Реестр всех выявленных замечаний и ошибок в ходе тестирования.
2.2. Документальное подтверждение устранения критичных и высокоприоритетных замечаний.
2.3. Обновленная конфигурация ИТ-систем после внесения корректировок.
2.4. Протоколы повторного тестирования (регрессионного тестирования) исправленных элементов.

3. Готовность системы к переходу в промышленную эксплуатацию:
3.1. Подтверждение соответствия внедренной ИТ-архитектуры техническим и бизнес-требованиям.
3.2. Успешное прохождение всех запланированных видов тестирования.
3.3. Положительные результаты UAT от представителей бизнес-пользователей.
3.4. Устранение всех критических и высокоприоритетных замечаний.
3.5. Готовность эксплуатационной документации и обученного персонала.
3.6. Формальное одобрение перехода в промышленную эксплуатацию от ответственных лиц/комитета.

Этап 6: Переход в Промышленную Эксплуатацию и Поддержка

Цель: Перевести ИТ-инфраструктуру в режим полноценной эксплуатации и обеспечить её поддержку.

Деятельность:

1. Go-Live Plan (План перехода в промышленную эксплуатацию):
   1.1. Разработка детального плана запуска (Go-Live Plan):
      - Определение точной даты и временного окна перехода (окно обслуживания).
      - Составление пошаговой процедуры переключения с текущей (если есть) на новую ИТ-инфраструктуру.
      - Подробное описание процедур отката на случай возникновения критических проблем во время перехода.
      - Планирование миграции пользовательских данных и профилей (если требуется).
   1.2. Назначение ответственных:
      - Формальное определение ответственных лиц за каждый этап и аспект перехода (технический руководитель, представители бизнеса, ИТ-специалисты, представители подрядчиков).
      - Создание списка контактных лиц для экстренной связи.
   1.3. Коммуникация плана Go-Live:
      - Информирование всех заинтересованных сторон (пользователей, ИТ-персонала, руководства) о дате, времени, ожидаемом влиянии и плане перехода.
      - Подготовка и распространение инструкций для пользователей на период перехода.

2. Планирование и выполнение перехода на новую инфраструктуру:
   2.1. Переезд (если применимо):
      - Физический переезд оборудования, документов, персонала в новое здание/помещение.
      - Координация логистики, безопасности и связи во время переезда.
   2.2. Переключение пользователей:
      - Перевод пользовательских рабочих мест на новую ИТ-инфраструктуру (изменение сетевых настроек, предоставление доступа к новым ресурсам).
      - Обеспечение доступа к приложениям и данным через новую архитектуру.
   2.3. Миграция данных:
      - Выполнение финальной миграции актуальных данных (если не была завершена ранее).
      - Проверка целостности и доступности данных после миграции.
   2.4. Финальные проверки:
      - Проведение финальных тестов работоспособности ключевых сервисов и приложений.
      - Убедиться в корректной работе всех интеграций.
      - Проверить работу систем мониторинга и ИБ.

3. Активное сопровождение в начальный период после перехода:
   3.1. Организация режима повышенной готовности:
      - Назначение дежурных ИТ-специалистов и поддержки подрядчиков на период после Go-Live.
      - Установка ускоренных каналов связи для оперативного реагирования.
   3.2. Мониторинг состояния системы:

- Усиленный контроль ключевых метрик производительности, доступности и безопасности.
- Быстрое реагирование на алерты и инциденты.

3.3. Решение инцидентов первой необходимости:
- Оперативное устранение проблем, возникающих у пользователей или в инфраструктуре сразу после перехода.

4. Обучение администраторов/пользователей:
4.1. Проведение тренингов по новым системам и процессам:
- Организация и проведение обучающих сессий для ИТ-администраторов по управлению новой инфраструктурой.
- Проведение тренингов для конечных пользователей по работе с новыми или обновленными приложениями, сервисами (почта, файлы, IP-телефония).

4.2. Предоставление обучающих материалов:
- Разработка и распространение инструкций, руководств пользователя, FAQ.
- Обеспечение доступа к электронным обучающим ресурсам (если созданы).

5. Передача документации и знаний службе поддержки (ITSM):
5.1. Передача эксплуатационной документации:
- Передача всей подготовленной документации (руководства администратора, инструкции, схемы, политики) ответственным лицам ИТ-отдела.
- Обеспечение структурированного хранения документации.

5.2. Передача знаний:
- Проведение сессий передачи знаний (knowledge transfer) от проектной команды (внутренней и внешней) ИТ-персоналу, который будет осуществлять поддержку.
- Обучение персонала работе с ITSM-процессами и инструментами, настроенными в рамках проекта.

6. Запуск регулярных процессов мониторинга, резервного копирования, обновлений:
6.1. Запуск регулярных процессов мониторинга:
- Полноценный запуск системы мониторинга, определенной на Этапе 2.
- Установление регулярных отчетов о состоянии ИТ для ИТ-менеджмента.

6.2. Запуск регулярных процессов резервного копирования:
- Обеспечение регулярного выполнения заданий резервного копирования.
- Мониторинг успешности выполнения бэкапов.

6.3. Планирование и выполнение регулярных обновлений:
- Разработка графика регулярных обновлений ОС, ПО, микрокода оборудования.
- Установление процесса тестирования и применения обновлений с минимальным влиянием на бизнес.

7. Post-Implementation Review (PIR):
7.1. Анализ результатов проекта:
- Сравнение фактических результатов проекта с запланированными целями и KPI.
- Оценка соответствия реализованной архитектуры исходным требованиям.

7.2. Выявление отклонений от плана, причин и извлеченных уроков:
- Анализ отклонений по срокам, бюджету, качеству.
- Идентификация причин успехов и неудач в ходе проекта.
- Формулирование уроков learned для применения в будущих проектах.

8. Передача в эксплуатацию:
8.1. Формальная передача системы в эксплуатацию:
- Подготовка и подписание акта сдачи-приемки ИТ-инфраструктуры.
- Официальное уведомление заинтересованных сторон о переходе системы в штатную эксплуатацию.

8.2. Передача ответственности:
- Формальная передача ответственности за эксплуатацию, поддержку и развитие ИТ-инфраструктуры ИТ-отделу заказчика.
- Уточнение ролей и границ ответственности между внутренней командой и внешними подрядчиками (если остались).

9. Закрытие проекта:
9.1. Финальный анализ результатов:
- Подведение итогов проекта, оценка достигнутых результатов.
- Формирование окончательного отчета о проекте.
9.2. Документирование уроков learned:
- Фиксация ключевых уроков и рекомендаций в формализованном виде.
9.3. Архивирование проектной документации:
- Сбор и передача всей проектной документации в архив предприятия.
9.4. Освобождение ресурсов:
- Освобождение временно задействованных ресурсов (персонал, оборудование тестовой среды).
- Завершение контрактов с подрядчиками, чья работа полностью завершена.

Результат Этап 6:

1. ИТ-инфраструктура, находящаяся в управляемой эксплуатации:
1.1. ИТ-инфраструктура полностью функционирует и обслуживает бизнес-процессы предприятия.
1.2. Все ключевые сервисы и приложения доступны пользователям.
1.3. Инфраструктура находится на гарантийном обслуживании (если применимо).
1.4. Работают процессы мониторинга, резервного копирования, управления инцидентами (ITSM).

2. Документация по эксплуатации:
2.1. Переданная и структурированная эксплуатационная документация.
2.2. Документация по ITSM-процессам и используемым инструментам.
2.3. Актуальные схемы ИТ-архитектуры и инвентаризация CI (CMDB).
2.4. Политики и регламенты ИТ.

3. Закрытый проект:
3.1. Подписанный акт сдачи-приемки проекта.
3.2. Формальный отчет о завершении проекта с анализом результатов.
3.3. Документ "Уроки Learned" (Lessons Learned).
3.4. Архив проектной документации.
3.5. Освобождение проектных ресурсов и завершение контрактов с подрядчиками.

Дополнительные общие аспекты:

1. Управление проектом:
   1.1. Использование методологии:
   - Определение и применение подходящей методологии управления проектом (Agile, Waterfall, Hybrid) в зависимости от специфики задач и требований заказчика.
   - Адаптация выбранной методологии под специфику ИТ-проекта (итерации, спринты, фазы, контрольные точки).

   1.2. Регулярные встречи:
   - Организация и проведение регулярных встреч проектной команды (ежедневные stand-up, еженедельные планерки).
   - Проведение статусных встреч с заказчиком и ключевыми заинтересованными сторонами (еженедельно/ежемесячно).
   - Организация тематических встреч по управлению рисками, качеством, изменениями.

   1.3. Отчетность по прогрессу:
   - Подготовка и предоставление регулярной отчетности о ходе проекта (прогресс выполнения задач, расходование бюджета, статус рисков).
   - Использование дашбордов и визуальных инструментов для отслеживания ключевых метрик проекта.
   - Подготовка итоговых отчетов по завершению ключевых этапов и проекта в целом.

   1.4. Управление изменениями в рамках проекта:
   - Установление формализованного процесса управления изменениями (Change Control Process).
   - Рассмотрение, оценка влияния, одобрение или отклонение запросов на изменение scope проекта.
   - Документирование всех утвержденных изменений и их влияния на план, бюджет и сроки.

2. Соблюдение стандартов и регулирования:
   2.1. Учет отраслевых стандартов:
   - Идентификация и применение соответствующих отраслевых стандартов (например, ISO 27001 для информационной безопасности, ISO 20000 для ITSM, ISO 7000/14000 для устойчивого развития).
   - Интеграция требований стандартов в процессы проектирования, внедрения и эксплуатации ИТ-архитектуры.
   - Планирование мероприятий по аудиту соответствия стандартам.

   2.2. Соблюдение законодательных требований:
   - Обеспечение соответствия проекта и реализованной ИТ-архитектуры действующему законодательству (законы о персональных данных, законодательство в области связи, отраслевые регуляторные требования).
   - Учет требований по локализации данных и обработке персональной информации.
   - Обеспечение выполнения требований по отчетности перед регулирующими органами, если применимо.

3. Устойчивость и экологичность:
   3.1. Рассмотрение вопросов энергоэффективности:
   - Выбор энергоэффективного оборудования (серверы, СХД, сетевое оборудование) при закупке.
   - Проектирование инфраструктуры с учетом минимизации энергопотребления.
   - Мониторинг и оптимизация энергопотребления в ходе эксплуатации.

   3.2. Утилизация старого оборудования:

- Планирование и организация безопасной и экологически responsible утилизации списываемого ИТ-оборудования.
- Выбор сертифицированных компаний для утилизации электронных отходов.
- Обеспечение уничтожения носителей информации перед утилизацией для защиты конфиденциальных данных.
- Документирование процесса утилизации.