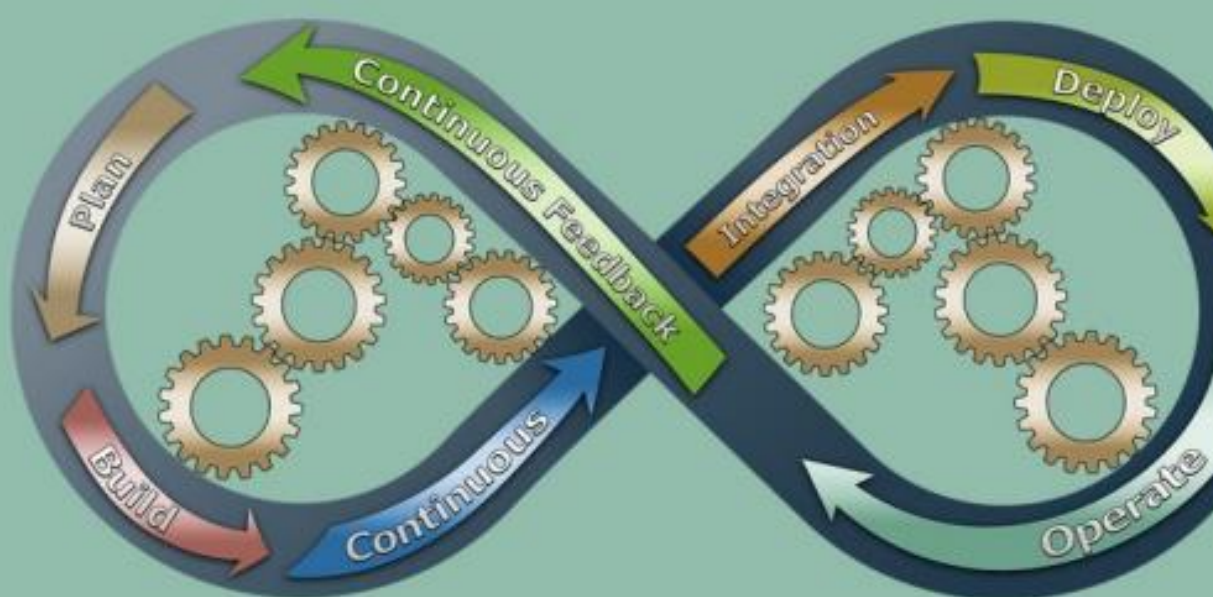


Вадим Алджанов
ИТ-архитектура от А до Я: Теоретические основы. Первое
издание

Вадим Алджанов



ИТ-АРХИТЕКТУРА ОТ А ДО Я: ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

Первое издание

http://www.litres.ru/pages/biblio_book/?art=33169575
ISBN 9785449081988

Аннотация

В книге собраны и обобщены теоретические знания в таких областях ИТ, как архитектура предприятия, информационной безопасности, управление сервисами, проектами, бизнес-процессами. Даются описание модели и подходы по расчету стоимости владения и организационные аспекты управления ИТ. Книга будет полезна менеджерам и руководителям ИТ. Материал изложен в логической последовательности для методичного изучения всех аспектов деятельности ИТ, наряду с использованием в качестве справочного пособия.

ИТ-архитектура от А до Я: Теоретические основы Первое издание

Вадим Алджанов

© Вадим Алджанов, 2018

ISBN 978-5-4490-8198-8

Создано в интеллектуальной издательской системе Ridero

Предисловие

Об Авторе



Вадим Алджанов (англ. Vadim Aldzhanov) [Microsoft MCP, MCSA Security, MCSE Security, MCTS, MCITP, MCITP SQL Database Administrator, Cisco CCNA, VMware VCP4, CompTIA A+, Network+, Security+, EC—Council CEH и ECSA, SNIA Certified Storage Professional SCSP, Wireless Technology CWTS, CWNA, CWSP, IT Management ITILv3, Apple Certified Associate – Integration | Management].

В серии книг «ИТ Архитектура от А до Я» собраны и обобщены знания и опыт за более чем 17+ лет работы в ИТ. В течении 14 лет проработал в банковской сфере, большую часть времени на позиции руководителя ИТ департамента. На данный момент являюсь ИТ Архитектором в одном из крупных холдингов страны. Имею степень бакалавра по специальности «Радиотехника» и степень магистра по направлению «Компьютерные Информационные Системы (CIS)». На данный момент продолжаю образование на получение докторской степени по направлению «Менеджмент Информационных Систем (MIS)». Кроме этого имеется порядка тысячи часов обучения на специализированных курсах по направлениям системное администрирование, компьютерные сети, беспроводные сети, системы хранения, системы виртуализации, информационная безопасность, управление ИТ сервисами, управление проектами, банковское дело, пластиковые карты, стратегическое планирование, проведение аудита и прочие. Профиль в LinkedIn: <https://www.linkedin.com/in/vadim-aldzhanov-623a7b44/>

Введение

Серия книг «ИТ Архитектура от А до Я» является попыткой автора собрать, обобщить и систематизировать накопленный опыт и знания в ИТ области.

Серия книг «ИТ Архитектура от А до Я» – Зеленая книга

Издание «ИТ Архитектура от А до Я: Теоретические основы». Первая книга серии «ИТ Архитектура от А до Я» содержит теоретические основы планирования, построения и сопровождения ИТ архитектуры, управления Проектами, ИТ сервисами и т.п. В качестве источника используются как проверенные на практике материалы, так и рекомендации стандартов и практик. Является переработанным, исправленным и дополненным изданием «ИТ Архитектура: практическое руководство от А до Я».

Серия книг «ИТ Архитектура от А до Я» – Синяя книга

Издание «ИТ Архитектура от А до Я: Комплексное решение». Вторая книга серии «ИТ Архитектура от А до Я» содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе основ теории, описанной в первой книге. В качестве примеров рассмотрены решения, на базе Windows 10/2016, комплексного решения по мониторингу, управлению и конфигурированию Microsoft System Center 2016, портал Microsoft SharePoint Server 2016, решения по управлению проектами Microsoft Project Server 2016, почтовый сервер Exchange 2016, решение Skype for Business 2015, функциональные возможности Direct Access 2016, Hyper-V, DFS и File Server, RDS и т.п. Представлены детальные требования и примеры расчетов по системам обеспечения. Приведены расчёты мощности и стоимости решений. В качестве примеров используются решения, которые выбраны автором как наиболее подходящие для выполнения поставленных задач, популярные или с которыми автор знаком на практике. Является переработанным, исправленным и дополненным изданием «ИТ Архитектура: практическое руководство от А до Я».

Серия книг «ИТ Архитектура от А до Я» – Серая книга

Издание «Шаблоны ИТ документов». Сборник содержит набор шаблонов и примеров документации, необходимой в повседневной деятельности ИТ. В качестве источника используются как проверенные на практике материалы, так и рекомендации стандартов и практик.

Серия книг «ИТ Архитектура от А до Я» – Желтая книга

Издание «Каталог ИТ решений». Сборник содержит описание возможностей различных

ИТ решений, анализ и сравнения функциональных возможностей. На текущий момент протестированы или использованы на опыте более сотни решений.

Серия книг «ИТ Архитектура от А до Я» – Красная книга

Издание «Альтернативное решения». Книга серии «ИТ Архитектура от А до Я» содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе теории, описанной в книге «ИТ Архитектура от А до Я: Теоретические основы». В качестве примеров используются решения, приоритетный критерий выбора которых является «нулевая стоимость». В качестве базового решения принимается ИТ инфраструктура и компоненты, описанные в «Синей книги».

Серия книг «ИТ Архитектура от А до Я» – Черная книга

Издание «Облачное решение». Книга серии «ИТ Архитектура от А до Я» содержит детальную техническую информацию и практические примеры реализации ИТ решений на основе теории, описанной в книге «ИТ Архитектура от А до Я: Теоретические основы». В качестве примеров используются по возможности «облачные» решения.

Цели книги

Цель книги, помочь специалистам, руководителям и директорам ИТ в построении Архитектуры Предприятия, организации процессов управления, расчете стоимости внедрения и сопровождения ИТ инфраструктуры, в выборе оптимального архитектурного решения, как с точки зрения бизнеса, так и с точки зрения ИТ. Книга поможет организовать коммуникацию между бизнесом и ИТ, позволив им общаться на одном «языке». Материала, изложенного в книге недостаточно для детального изучения всех аспектов деятельности ИТ, но достаточно для понимания связей различных аспектов и задания вектора развития организации в целом и ИТ в частности.

Книга не является обязательным руководством по выбору того или иного продукта или решения, а выражает точку зрения автора.

Материал изложен в логической последовательности, дополнен теоретическими сведениями и снабжен наглядными примерами реализации. Это дает возможность использования данного руководства для методичного изучения всех аспектов деятельности ИТ, наряду с использованием его в качестве справочного пособия при работе с конкретными системами.

Сферы, охваченные книгой

Книга является первой из серии «ИТ Архитектура от А до Я» и представляет собой руководство на русском языке, в котором собраны и обобщены теоретические знания, в области построения Архитектуры Предприятия, Управления Проектами, Информационной Безопасности, Организации и Управления ИТ сервисами и ИТ аудита, так и рассмотрена последовательность применения их на практике, позволяющий полностью обеспечить потребности организации в процессе создания и управления ИТ архитектурой и инфраструктурой. На основе обширного материала, дается систематичное описание современного состояния ИТ компании, приводятся основные модели и подходы по формированию ИТ стратегии, управлению проектами, управлению ИТ сервисами, анализу рисков и управлению качеством, Контроль и аудит ИТ, интеграции и взаимодействие различных подходов и методов.

Книга предназначена для широкого круга читателей и будет полезна:

Топ-менеджерам, кураторам ИТ, ИТ директорам крупных и средних компаний так как позволит лучше понимать Архитектуру Предприятия (Enterprise Architecture) на базе подхода (TOGAF), роль и вовлеченность ИТ в бизнес. Показатели распределения финансовых инвестиций на ИТ сервисы. Представители бизнеса смогут понять общие аспекты по функционированию ИТ инфраструктуры, технические термины, принципиальные отличия

различных архитектурных решений, принципы построения и сопровождения технических решений. Позволяет сформировать понимаемые обоими сторонами метрики и отчеты по оценке эффективности и результативности функционирования ИТ инфраструктуры.

Руководителям ИТ подразделений, ИТ архитекторам, менеджерам среднего звена ИТ департамента, а также менеджерам проектов книга предоставляет теоретические основы управления ИТ сервисами (ITSM) с применением рекомендаций практик ITIL, интеграцию методики Управление Проектами (PMI) в ИТ, вопросы аудита ИТ (CobiT) и Информационной Безопасности.

Книга не предназначена для малых ИТ инфраструктур т. к. стоимость бумаги выше чем требования, предъявляемые к ИТ. Так же будет мало эффективна для крупных предприятий с корпоративным управлением т. к. по каждому направлению деятельности скорее всего имеются узко направленные эксперты.

Благодарность

Выражаю благодарность друзьям, учителям, руководителям и коллегам за помощь в написании книги, а также бесценный опыт и знания полученный от общения с такими людьми как Александр Буслаев («AIG Group»), Иршад Гулиев («SINAM»), Фазиль Маммедов («ROTABANK»), Яна Хмельницкая и Karsten Stellner («LFS Financial Systems GmbH»), Thomas Engelhardt («Microfinance Bank of Azerbaijan»), Andrew Pospelovsky («ACCESSBANK») и Alan Crompton («Baku European Games Operation Committee BEGOC 2015»).

Юридическое уведомление

Информация, содержащаяся в книге, не несет в себе никакой коммерческой тайны или иной конфиденциальной информации. Материалы собраны из открытых источников, переработаны автором, используя имеющийся опыт и знания. Некоторые рассмотренные примеры приведены только для справки и являются вымышленными. Любое сходство с реально существующими людьми или организациями является случайным. Все упоминающийся в книге названия компаний и продуктов могут быть торговыми марками, принадлежащими соответствующим владельцам.

Авторские права

Информация, указанная в книге не может воспроизводиться, дублироваться, копироваться, передаваться, распространяться, храниться или использоваться иным образом для любого коммерческого и не коммерческого использования без письменного согласия автора.

@ Copyrights Vadim Aldzhanov, 2018

Отказ от ответственности

Автор не дает никаких гарантий или заявлений о точности, пригодности или полноте информации, ссылок или других предметов, которые содержатся в настоящем документе. Книга доступна всем читателям «как есть» без каких-либо заявлений или гарантий любого рода, явных или подразумеваемых, включая гарантии в отношении товарности или пригодности для определенной цели. Документ может содержать неточности или орфографические ошибки.

Автор не несет никакой ответственности за прямые, косвенные, случайные или прочие убытки при использовании данного руководства. Читатель данного руководства проинформирован.

Посвящается моим родителям, любящей жене и двум прекрасным дочерям.

Теоретические Основы

Первая книга серии включает в себя рассмотрение теоретических основ по построению ИТ компании. В частности, рассмотрены:

Глава 1: Концепции построения Архитектуры Предприятия – В данной главе рассматриваются вопросы построения Архитектуры Предприятия, построения ИТ стратегии и т.п.

Глава 2: Концепция Управления Проектами – в главе рассматриваются основы Управления Проектами, применяемые методологии, принятые методы и т.п.

Глава 3: Концепция Управления Рисками – в главе рассматриваются методики и методы оценки рисков, классификация рисков и типы реагирования на риски.

Глава 4: Концепция Управления Качеством – в главе рассмотрены базовые принципы и методы управления проектами при использовании методов, основанных на принципах управления качеством и бережливого производства.

Глава 5: Концепция Управление Бизнес Процессами и Модели Деловой Активности различных сфер бизнеса, Рассмотрены основы построения бизнес процессов, виду организации бизнеса и связь с информационными системами.

Глава 6: Концепция Информационных Систем и Интеграции Данных – В данной главе рассмотрены вопросы по интеграции данных между различными информационными системами, различные архитектурные решения, проблемы и возможности. Рассмотрены уровни централизации Автоматизированных Систем Управления.

Глава 7: Концепция Информационной Безопасности – Рассмотрены вопросы информационной безопасности, порядок организации взаимодействия информационной безопасности и ИТ.

Глава 8: Концепция Управления ИТ сервисами – Рассмотрены процессы построения управления ИТ сервисами с применением практики ITIL.

Глава 9: Концепция Контроля и аудита ИТ – рассмотрены общие вопросы по контролю ИТ и проведению аудита

Глава 10: Концепция Финансирования ИТ – Рассмотрены модели финансирования, принципы оценки ИТ проектов, методы и практики расчета стоимости ИТ сервисов и т.п.

Глава 11: Организация деятельности ИТ – рассмотрены общие вопросы по структуре, организации, управлению ИТ департаментом

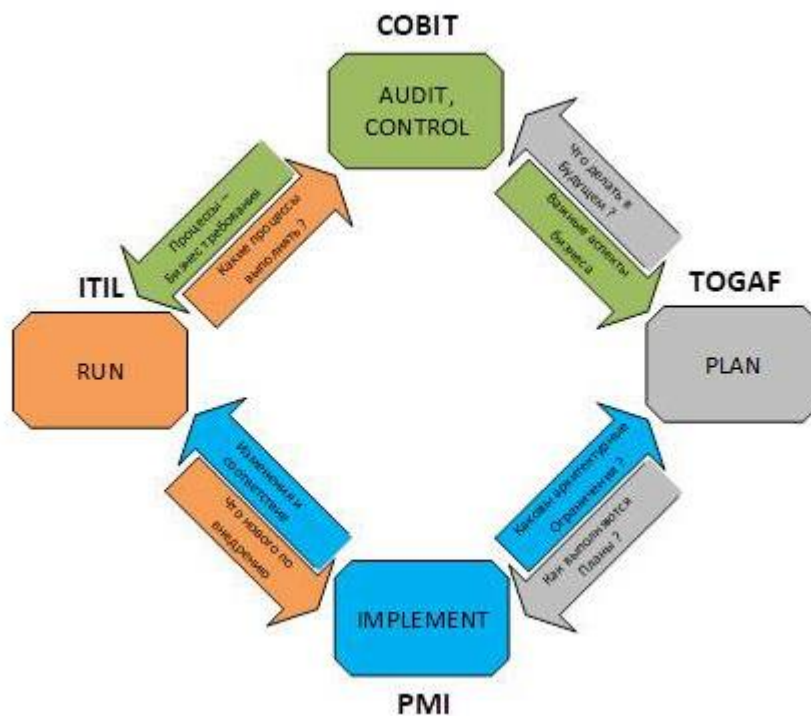
Глава 12: Компоненты ИТ инфраструктуры – рассмотрены высокоуровневые компоненты ИТ инфраструктуры.

Глава 13: Компоненты Систем Обеспечения ИТ – рассмотрены высокоуровневые компоненты инженерных систем и систем обеспечения.

Концепция Архитектуры Предприятия

Общие Положения

В данной главе описывается общая информация по Архитектуре Предприятия (Enterprise Architecture). Обобщенное определение можно представить, как:



Архитектура Предприятия – это набор принципов, методов и моделей, который используется в проектировании и реализации организационной структуры, бизнес-процессов, информационных систем и технологий. Она представляет из себя управленческую практику, направленную на максимизацию отдачи от ресурсов предприятия, инвестиций в ИТ, деятельности по разработке систем в процессе достижения целей предприятия, перевод видения и стратегии бизнеса в эффективное изменение компании посредством создания, обсуждения и улучшения ключевых требований и принципов, которые описывают будущее состояние компании и делают возможным её развитие.

Так как Архитектура Предприятия представляет из себя сложное и комплексное решение, включающая в себя переплетение различных методологий и техник, при построении Архитектуры Предприятия должны быть учтены, но не ограничены, рекомендациями следующих стандартов:

TOGAF – Enterprise Architecture
 ISO/IEC 20000 – Quality in IT Service Management
 ISO/IEC 27000 – Best Practice IT Security Standards
 CobiT v5 – Audit and Control Framework
 ITIL v3 – Best practices in IT Service Management
 MOF – Microsoft Operations Framework
 PMI – Project Management Institute

Архитектура призвана ответить на такие вызовы и проблемы организации как:

- Недовольство бизнеса ИТ-службой. Причины могут быть объективные или субъективные.
- Невозможность оценить эффективность использования информационных технологий в бизнесе.
- Отсутствие порядка в «зоопарке» ИТ решений и систем, внедренных в организации.
- Сложность принятия решений, связанных с информационными технологиями
- Сложность согласование ИТ-бюджета и запуск ИТ-проектов.
- Рост ценности «Информации» и связанности бизнеса и ИТ.
- Отсутствие прозрачных и понятных связей бизнеса и ИТ?
- Можно ли решить актуальные задачи бизнеса с использованием ИТ?

- Как заставить ИТ давать компании большую ценность?
- Как нужно менять ИТ при изменениях в бизнесе?
- ИТ системы сложны, не управляемы и дороги в обслуживании
- ИТ системы сдерживают организацию от адекватного реагирования на изменения в бизнесе
- Критичная для бизнеса информация не своевременна и не адекватна
- Отсутствует культура общения бизнеса и ИТ

Как результат бизнес не видит ценности в информационных технологиях. ИТ директору тяжело продвинуть новые идеи, если он говорит о технологиях. Его не понимают. Все, что ему остается, это поддерживать то, что есть, и делать те задачки, которые подбрасывает бизнес. Возникают серьезные сложности с обоснованием ИТ бюджетов. ИТ директор по факту больше похож на прораба, латающего дыры, а не на топ менеджера, который работает над развитием компании. Топ менеджеры быстро теряют интерес к ИТ проектам, как следствие, теряют финансирование и проваливаются. На место ИТ департамента приходят различные системные интеграторы по внедрению «супер-пуперских» решений, которые «спасут» бизнес. Или возникают идеи забрать все ИТ активы и услуги компании и передать на аутсорсинг. Бороться ИТ департаменту с интеграторами будет сложно и результат будет предсказуем, ключевая компетенция у интеграторов одна – технологии, и здесь им равных нет. ИТ департамент превращается в «болото», и его покидают лучшие сотрудники, а вместе с ними будут утеряны уникальные знания и навыки. Цели у интегратора или аутсорсинг компании такая же, как и у вашей компании – получение прибыли. Но в отличие от ИТ департамента, интересы которого совпадают с интересами вашей компании, интересы интегратора могут не совпадать с вашими интересами, или уникальными идеями и видением. В лучшем случае будет «как у всех», и бизнес потеряет идентичность (если он неразрывно связан с ИТ) или говоря словами персонажа одного из кинофильмов: «... будет все у нас все по-новому оставаясь все по-старому...». Конец печален.

Основные аспекты Архитектуры Предприятия

Для борьбы с выше сказанными проблемами и последствиями, Архитектура Предприятия помогает сформулировать следующие важные критерии.

Определение Структуры Предприятия

При построении Архитектуры Предприятия самый первый и наиболее важный аспект – понимание организационной структуры предприятия, принципов управления, принятия решения и т.п.

Структура организации – фиксированное упорядоченное множество объектов и связей между ними.

По характеру специализации и видам деятельности различают:

- Вертикальное разделение – по уровню подчинения
- Горизонтальное разделение – по функциям и специфике деятельности

Соответственно в структуре управления различают линейные связи по типу «начальник – подчинённый» и функциональные «профессиональная интеграция на основе специфики деятельности». Как результат, тип структуры организации можно представить, как следующие основные типы и их разновидности:

- Плоская – наиболее простая структура. Подходит для рабочих или проектных групп, или небольшой организации.
- Иерархическая (бюрократическая) – формирование структуры исходя из структуры организации, разделение труда на функции и ответственности работников.

- Линейная – управление по прямой (руководитель – подчинённый), общение между подразделениями только через руководителей подразделений

- Функциональная – взаимодействие идет по функциональному признаку

- Линейно-функциональная – взаимодействие совмещается по линейному и функциональному типу (наиболее используемая модель)

- Линейно-штабная – отдельные функциональные группы (штабы), самостоятельно ведущие работу с подразделениями или организациями. Как пример группа компаний в составе холдинга.

- Дивизионная – характеризуется центральной координацией с децентрализованным управлением. Ключевые фигуры в данном случае не руководители функциональных подразделений, а менеджеры отдельных объединений (менеджеры филиалов, заводов и т.п.)

- Органические (адаптивные) – формирование структуры исходит из необходимости приспособления к изменениям. Отношения формируются, исходя не из структуры, а характера поставленных задач.

- Проектные – организуется при ведении проектов

- Матричные (программно-целевые) – принцип двойного подчинения, непосредственное подчинения руководителю, и проектному менеджеру

- Бригадные (кросс-функциональные) – работа обособленными группами, с самостоятельным управлением и принятием решений (противоположность иерархическому типу)

Существование той или иной организационной структуры может зависеть от ряда факторов:

- Специфика и степень разнообразия деятельности

- Географическое размещение

- Уровень централизации в организации

- Стратегия организации

- Количества и спектра предоставляемых услуг

Определение роли ИТ в составе организации

Одним из главных критериев при построении Архитектуры Предприятия можно выделить задачу по определению роли ИТ в составе организации. Если отбросить множество статей, рекомендаций различных консультантов о значимости ИТ в современном мире и «бла бла бла», необходимо четко и конкретно зафиксировать роль ИТ в составе организации, задачи, права возможности и степень ответственности.

Для понимания роли ИТ в конкретной организации нужно ответить на следующие вопросы:

Вовлеченность ИТ в бизнес организации. Насколько бизнес организации зависит от ИТ. Многие бизнес процессы и функции завязаны на сложных, централизованных или специфических ИТ решениях. Развитие бизнеса невозможно без быстрой и качественной работы ИТ. Есть целые отрасли, которые зависят от ИТ: банки, страховщики, прочие финансисты, сервисные компании, госорганы, технологические компании, энергетика и прочие (как пример в банке две трети сотрудников так или иначе работают с централизованной банковской программой, в то время как для сельского хозяйства, лишь небольшая часть организации использует ИТ решения, да и те по большей части автономные – большинство сотрудников работают на поле или уровень компьютеризации компании низкий).

Вашу организацию можно отнести к крупному или среднему бизнесу. На мой взгляд, до тех пор, пока все технологии компании со всеми подробностями помещаются в одной голове, а ИТ директор напрямую общается с руководством организации об архитектуре предприятия думать рано. Для малого бизнеса архитектура предприятия вообще, как телега пятое колесо.

Компания активно развивает ИТ. В компании идет несколько ИТ проектов в год, или хотя бы один проект по внедрению ERP, CRM или прочего сложного решения. Формирование Архитектуры Предприятия поможет с принятием решений и убережет от большинства переделок, ошибок, не состыковок, задержек и прочих проблем. У кого-то, и желательно не одного, должна быть общая картинка будущего и понимание процесса развития. Иначе кусочки мозаики, созданные в разных проектах, не сойдутся.

У компании периодически происходят кризисы в ИТ, которые имеют существенное влияние на бизнес. В информационных системах происходят сбои, которые негативно влияют на бизнес, вплоть до его остановки. Сбои вызваны проблемами в интеграции, просчетами в инфраструктурных решениях, временными решениями и просто бардаком. Не все проекты, в том числе и ИТ, заканчиваются успешно, уложившись в сроки, бюджет и заявленные требования. Если руководство вашей компании устало от провалов, задержек, превышения бюджетов ИТ проектов, то стоит задуматься.

Компании важна скорость, качество и эффективность развития ИТ. Одна из сторон (Бизнес или ИТ) развивается значительно быстрее чем другая. В случае, если бизнес развивается быстрее чем ИТ, то ИТ становится тормозом в развитии компании. И наоборот, если ИТ развивается быстрее чем необходимо бизнесу, то владельцы бизнеса несут убытки как финансовые (хорошее ИТ стоит денег), так и упущенная прибыль (бизнес не использует все потенциальные возможности ИТ). Необходимо организовать работу обеих сторон «на одной волне» для гармоничного развития всех элементов компании.

Выстраивание взаимоотношения между бизнесом и ИТ

Сфокусировать действия ИТ на целях и задачах бизнеса. Бизнес и ИТ стороны по-разному видят задачи, цели и ожидания по отношению друг к другу. Видение ИТ сотрудников «... мы прекрасно разбираемся в технологиях, нам платят деньги за умение программировать, настраивать, устанавливать и решать технические проблемы и т.п. Наша работа начинается после получения технического задания...». Видение со стороны бизнеса – «... столько новых ИТ технологий, ИТ должен нам внедрить нам какое-то решение, чтобы увеличить объем продаж. Или что еще хуже, нам нужно решение XXX, оно есть у конкурентов и поэтому продажи у них выше... внедряйте мы уже все решили вы ничего не понимаете бизнесе...». Задача ИТ директора, участие на равных в обсуждении стратегии бизнеса. Общие принцип можно определить, как: «бизнес описывает свои требования и ожидания (Бизнес требования), ИТ в свою очередь формирует техническое задание для достижения целей.»

Наладить сотрудничество между бизнесом и ИТ.

Из выше сказанного вытекает вторая важная проблема – «вакуум» в коммуникации между сотрудниками бизнеса и ИТ. Задача руководства организации, и ИТ директора в том числе, наладить общение между сотрудниками организации не только на высшем уровне, но и между сотрудниками среднего уровня, и непосредственных исполнителей бизнеса и ИТ. Как говорится в популярной фразе «дьявол кроется в мелочах». Любая классная идея в общих чертах должна быть спущена вниз для детальной проработки. На этом этапе особенности мышления ИТ специалистов с его жесткими связями «причина – следствие», вопросами «... что будет если ...», «... как контролировать...», «... как измерить...», анализ сценариев предельных состояний, поможет выработать оптимальное решение. Кроме этого такие вопросы помогут представителям бизнеса лучше понять и проработать решение, с точки зрения бизнеса. Понять, что можно требовать от ИТ, текущие возможности решения и их перспективные возможности или ограничения.

Получить максимальную ценность от ИТ.

Для большинства организаций, если только это не ИТ компания, ИТ является лишь инструментом достижения целей бизнеса, вторичным сервисом, таким же, как и бухгалтерия

или администрация, обеспечивающих сопровождение основных направлений и процессов. ИТ оценивает решения с точки зрения технической зрелости, законченности, функциональности и т. п. В то время как бизнес интересуется лишь возможностью извлечения прибыли. Идеально проработанное техническое решение может свести на «нет» бизнес-преимущества самой идеи, сделать ее сложной в эксплуатации пользователями, высокой стоимости как при внедрении, так и при сопровождении, что снижает финансовую выгоду, не удобную для клиентов и т. п. Задачи ИТ-директора – разработка не самого «лучшего» решения с точки зрения ИТ, а наиболее «правильного». Наиболее «правильное» решение будет сформировано формулой и из следующих ключевых составляющих:

ЦЕННОСТЬ = ВЫГОДА – ЗАТРАТЫ

С точки зрения бизнеса: Получить максимальную ценность от ИТ. Ценность информационных технологий – это разница между выгодами использования информационных технологий и затратами на них).

С точки зрения ИТ: Соблюдение ИТ-ценностей и требований (технологичность, безопасность и управляемость ИТ).

Перенос части работ на сторону ИТ-департамента, или отказ от автоматизации ряда элементов, может снизить стоимость решения, повысить простоту эксплуатации и удобство для клиентов.

Одна из первоочередных задач – определить границы, где можно искать возможности, а где та грань, переход которой ломает основы управляемости ИТ и информационной безопасности.

Управлять изменениями

В контексте данной главы имеется в виду готовность к изменениям инициаторами которых является бизнес. Обстановка в бизнесе может меняться быстро и радикально. Появление новых ниш для бизнеса, разработка новых продуктов, слияния и поглощения и т. п. Это может привести к тому, что техническое решение, используемое в организации, перестает удовлетворять требованиям организации. Задача ИТ – адаптация имеющегося решения или разработка нового в кратчайшие сроки и с минимальным бюджетом для соответствия требованиям бизнеса. Как следствие при разработке ИТ-стратегии и ИТ-решений в частности, необходимо закладывать определенную гибкость и универсальность.

Навести порядок и управлять развитием ИТ.

Современные реалии ведения бизнеса и развития технологий приводят к тому, что бизнес требует внедрения все новых и новых технологических решений. Различные методы и модели их внедрения (самостоятельная разработка, покупка «коробочного» решения, внедрение и сопровождение со стороны третьей стороны и т. п.) приводят к тому, что в ИТ-инфраструктуре появляется большое количество различного аппаратного и программного обеспечения, частично дублирующего друг друга, устаревших решений, и т. п. Кроме этого, постоянная зависимость от специалистов, обладающих «уникальными» знаниями и опытом. Задача ИТ-директора – организация управления ИТ, непрерывное обучение сотрудников новым технологиям, выбор перспективных направлений, которые могут принести выгоду бизнесу.

Базовые принципы построения Архитектуры Предприятия

Комплексная автоматизация функции управления требует создания единого информационного пространства на любом современном предприятии, в котором обычные сотрудники и руководство смогут осуществлять свою деятельность, руководствуясь едиными правилами доступа, представления и обработки информации. Современные методы построения ЕИП предприятия базируются на проведении комплексного реинжиниринга бизнес-процессов, на создании информационно-логической модели и последующей

реализации соответствующего программного и информационного обеспечения с использованием новых технологий. Разработка ИТ-архитектуры позволяет ясно представить:

- Какая информация/данные критичны для бизнеса компании и как они организованы;
- Какие приложения будут поддерживать бизнес;
- Смогут ли эти приложения эффективно взаимодействовать между собой и с внешними системами партнеров и поставщиков;
- Соответствуют ли используемые технологии требованиям поддержки бизнес-процессов;
- Достаточно ли обеспечена информационная безопасность систем;
- Смогут ли сотрудники компании получить своевременный доступ к нужным данным из любого необходимого места;
- Какие стандарты должны использоваться при разработке и закупке компонент системы;

Формирование архитектуры производится с использованием распространенных методологий, рамочных моделей (frameworks) описания архитектуры и инструментальных средств моделирования (например, ARIS IT Architect) – с учетом имеющихся у Заказчика опыта и предпочтений. В ходе проекта формируется набор архитектурных принципов, определяются используемые и перспективные стандарты и разрабатываются модели архитектуры в целом и ее отдельных областей (приложения, данные, интеграция, техническая инфраструктура, безопасность и др.)

Примерный порядок построения единого информационного пространства предприятия следующий:

- Обследование предприятия**
 - °Цели и основные задачи;
 - °Четкое определение задач и целей проекта;
 - °Формулирование функционально-технических требований к проекту;
 - °Инфраструктурный аудит ИТ-системы предприятия для проектирования архитектуры решения;
 - °Формализация существующих на предприятии бизнес-процессов, автоматизируемых в рамках проекта;
 - °Получение данных для обоснования количества лицензий;
 - °Оценка ресурсов, которые потребуются для реализации проекта;
 - °Оценка рисков проекта;
 - °Разработка предварительного плана проекта, графика работ и спецификации поставок по каждому этапу и проекту в целом.
- Результаты обследования :**
 - °Отчет с фиксацией ситуации в виде «Как есть»;
 - °Предложение по созданию информационной системы в виде «Как необходимо»;
 - °Предложение по «Функционально-техническим требованиям к проекту»;
 - °План реализации проекта;
 - °Оценка рисков проекта и предложения по их минимизации;
 - °Ориентировочная стоимость пилотного проекта и конечного решения.
- Поставка необходимых предприятию аппаратного обеспечения и функциональных решений по автоматизации подразделений:**
 - °Адаптация и настройка базовых, при необходимости разработка новых решений в соответствии с функционально-техническими требованиями, полученными на этапе обследования;
 - °Развертывание платформы с базовыми сервисами обработки и хранения документов;
 - °Опытная эксплуатация решения;
 - °Интеграция с ERP-системой;

°Ввод системы в промышленную эксплуатацию.

•**Обучение технического персонала и пользователей.**

•**Обеспечение дополнительного функционала – работы, выделенные на этапе обследования в отдельные этапы.**

Архитектурный Фреймворк – это готовая методология и набор поддерживающих инструментов, которые адаптируются для использования в конкретной компании. В Фреймворке есть типовые архитектурные процессы, рекомендации по их адаптации для конкретной компании, рекомендации по формированию шаблонов архитектурных артефактов, требования к их заполнению, требования к архитекторам и многое другое.



Модель Архитектуры Предприятия можно разделить на несколько ключевых уровней (категорий):

Архитектура бизнеса – содержит стратегию компании, подход к управлению, организационную структуру и ключевые бизнес процессы.

Архитектура информационных систем – описывает, как устроены или будут устроены информационные системы компании. Архитектура информационных систем может быть разбита на две подгруппы:

Архитектура приложений – показывает бизнес приложения, развернутые в компании, их взаимодействие друг с другом, а также их связь с бизнес процессами компании

Архитектура данных – содержит описание логической и физической структуры данных компании, а также подход и средства управления данными.

Техническая архитектура – описывает программное обеспечение и оборудование, которое необходимо для развертывания бизнес сервисов, данные и приложения, ИТ инфраструктуру, сервера приложений, сети, телекоммуникации, стандарты и т. д.

Стратегии ИТ Архитектуры Предприятия		
Охват: все организация Уровень детализация: поверхностный		
Архитектура сегмента 1 Охват: бизнес подразделение, функция, направление Уровень детализация: средняя	Архитектура сегмента 2 Охват: бизнес подразделение, функция, направление Уровень детализация: средняя	Архитектура сегмента N Охват: бизнес подразделение, функция, направление Уровень детализация: средняя
Архитектура решения 1 Охват: ИТ-решение, Проект, бизнес-процесс, функция Уровень детализация: подробный	Архитектура решения 2 Охват: ИТ-решение, Проект, бизнес-процесс, функция Уровень детализация: подробный	Архитектура решения N Охват: ИТ-решение, Проект, бизнес-процесс, функция Уровень детализация: подробный

Следующим уровнем иерархии может быть по:

•**Стратегическая архитектура** описывает всю компанию в целом. На этом уровне вы не погружаетесь в особенности конкретных подразделений, направлений бизнеса и т. д. Стратегическая архитектура сконцентрирована на общих для всей компании стратегии, бизнес процессах, инвестициях, данных, системах и технологиях. Она прежде всего ориентирована на реализацию стратегии компании. На этом уровне определяются принципы и приоритеты, создаются общие для всей компании ИТ сервисы.

•**Архитектура сегмента**. Это архитектура направления деятельности компании, программы проектов или отдельного подразделения. Таких сегментов у компании будет несколько. На этом уровне вы погружаетесь в специфические особенности и требования конкретного подразделения, функции или компании в составе организации. Прорабатываете бизнес кейсы использования ИТ с руководством подразделения. Архитектура сегмента должна иметь ту же структуру и общие сервисы, что и стратегическая архитектура.

•**Архитектура решения** – архитектура конкретного ИТ решения. Она используется для реализации новых или доработки существующих ИТ решений сервисов или их частей. В ней учтены как общие для всей компании требования, так и специфические потребности, выявленные на уровне архитектуры сегмента. Рамки архитектуры решения ограничены одним проектом, процессов или функцией. Архитектура решения прорабатывается максимально детально. Это позволяет избежать неприятных сюрпризов в будущем при реализации проекта.

Уровни зрелости ИТ

В процессе роста и развития организации, департамент ИТ также проходит несколько этапов своего развития. При построении Архитектуры Предприятия следует принимать во внимание уровень зрелости организации в целом, так и ИТ в частности. Можно выделить следующие этапы и симптомы состояния ИТ департамента:

Начальный или «локализация»

В компании быстро разрабатывают или закупают информационные системы, которые дают ценность отдельным бизнес подразделением или функциям.

Основные симптомы данного этапа развития:

- Роль ИТ департамента – второстепенная
- Стратегия ИТ департамента – отсутствует
- Бюджет ИТ департамента – отсутствует
- Тип деятельности ИТ департамента – пассивный, только по запросу.
- Задачи менеджмента – максимальная экономия
- Место в организационной структуре компании – служба в составе бизнес

департамента (администрация, финансы)

Развития или «стандартизация»

Компания переходит от закрытия потребностей отдельных бизнес подразделений или функций и повышает эффективность ИТ за счет стандартизации технологий и инфраструктуры. Основные симптомы данного этапа развития:

- Роль ИТ департамента – не стратегический ресурс
- Стратегия ИТ департамента – отсутствует или на начальном уровне
- Бюджет ИТ департамента – отсутствует или управляемый со стороны
- Тип деятельности ИТ департамента – слабо активный по ИТ инфраструктуре и пассивный, только по запросу для бизнеса
- Задачи менеджмента – минимальные инвестиции
- Место в организационной структуре компании – служба или отдел в составе бизнес департамента (администрация, финансы) или под курацией.

Становления или «оптимизация»

Компания строит сквозные бизнес процессы, используя общие данные и информационные системы. Централизует по возможности бизнес процессы и функции подразделений в централизованных информационных системах по предварительно описанных операционных моделях. Основные симптомы данного этапа развития:

- Роль ИТ департамента – важная
- Стратегия ИТ департамента – частично отвечает бизнес требованиям
- Бюджет ИТ департамента – существует и управляем
- Тип деятельности ИТ департамента – реактивная реакция на бизнес требования,
- Задачи менеджмента – получение бизнес выгоды в краткосрочной перспективе
- Место в организационной структуре компании – выделенный департамент, но ИТ менеджер не входит в состав совета директоров.

Зрелый

Повторное использование имеющихся бизнес процессов и компонентов для создания новых сервисов и возможностей. ИТ работает на опережение и является не отъемлющей частью бизнеса. Основные симптомы данного этапа развития:

- Роль ИТ департамента – стратегический ресурс организации
- Стратегия ИТ департамента – интегрированная в бизнес стратегию компании
- Бюджет ИТ департамента – существует и рассматривается как инвестиции в бизнес
- Тип деятельности ИТ департамента – активная реакция (превентивная) на бизнес требования
- Задачи менеджмента – долгосрочные инвестиции в бизнес
- Место в организационной структуре компании – департамент, ИТ директор в составе совета директоров

Каждый из этих этапов имеет плюсы и минусы. Этап развития ИТ должен соответствовать этапу развития компании. Опыт показывает, что перескочить хотя бы через один из этапов сложно и требуются колоссальные затраты ресурсов (времени, денег, энергии сотрудников и т. д.), при этом эффект будет обратный. Большинство компаний проходят их один за другим. Переход на следующую стадию переходит при осознании руководством компании или остроты возникших вопросов:

- Проблемы поддержки роста и изменений бизнеса
- Дублирование бизнес процессов
- Многообразие платформ и систем
- Неудовлетворенность текущим состоянием ИТ

Критерии выбора методологии

Так как методологии сильно отличаются друг от друга, то следует задать критерии для их сравнения.

Полнота таксономии, определяет, насколько методология пригодна для классификации различных архитектурных артефактов. Полностью сосредоточена на фреймворке Захмана.

Полнота процесса, определяет, насколько детально представлен процесс создания архитектуры предприятия.

Руководство по эталонным моделям, определяет полезность методологии в создании адекватного набора эталонных моделей. На этом практически полностью сосредоточена методология FEA.

Практическое руководство определяет, насколько методология позволяет воплотить в жизнь умозрительное представление об архитектуре предприятия и сформировать культуру, в которой эта архитектура будет использоваться. На этом практически полностью сосредоточена методология Gartner.

Модель готовности определяет, насколько методология позволяет оценить эффективность использования архитектуры предприятия в различных подразделениях.

Ориентированность на бизнес определяет, ориентирована ли методология на использование технологии для повышения ценности бизнеса, где ценность бизнеса определяется как снижение затрат или увеличение доходов.

Руководство по управлению определяет, насколько методология полезна в понимании и создании эффективной модели управления для архитектуры предприятия.

Руководство по разбиению определяет полезность методологии в эффективном разбиении предприятия на отделы, что весьма важно при управлении сложностью.

Наличие каталога определяет, насколько эффективно методология позволяет создать каталог архитектурных активов, которые можно будет использовать в дальнейшем.

Нейтральность по отношению к поставщикам услуг определяет вероятность того, что при внедрении методологии вы окажетесь привязанными к конкретной консалтинговой организации. Высокая оценка означает низкую степень привязки к конкретной организации.

Доступность информации определяет количество и качество бесплатных или относительно недорогих материалов по данной методологии.

Время окупаемости инвестиций определяет продолжительность периода, в течение которого вы будете использовать данную методологию, прежде чем сможете построить на ее основе решения, обеспечивающие высокую ценность бизнеса.

Построение Архитектуры Предприятия может быть выполнено с применением различных методов и практик. В данной книге мы вкратце рассмотрим несколько и сфокусируем свое внимание на одной из них:

- «*Zahman Framework*» – наиболее ранняя и известная методология. Идеально подходит для «классификации» элементов архитектуры.

- «*TOGAF (The Open Group Architecture Framework)*». Методология получила широкую известность и распространение, во многом за счет открытости. Представляет из себя каркас «построения процессов».

- «*Gartner*» – методология экспертного анализа с использованием «лучших» практик.

- «*FEAF*» – методология построения архитектуры, использующая «сервис ориентированный» подход.

При построении ИТ Архитектуры Предприятия необходимо выделить следующие состояния архитектуры организации:

- Текущее состояние «As-is» или «Baseline Architecture».

- Переходное состояние «Transition Architecture».

- Будущее состояние «To-be» или «Target Architecture».

- План перехода «Enterprise Architecture Management Plan & Roadmap»

В общем случае Архитектура Предприятия представляет из себя план перехода от «Текущего» к «Будущему» состоянию организации. Архитектурный проект длится несколько лет и инициирует множество ИТ проектов. Эти проекты будут разной продолжительности, у них разные даты начала и окончания. Их нужно сгруппировать таким образом, чтобы изменения в бизнесе и ИТ происходили в нужное время, с минимальными рисками и без проблем с совместимостью. То есть архитектура может переходить из одного работоспособного состояния в другое несколько раз за время архитектурного проекта. Промежуточные состояния называют «переходной архитектурой» (Transition Architecture).

Архитектура Предприятия на основе методологии «ZAHMAN FRAMEWORKS»

Наиболее ранняя методология и на мой взгляд наиболее полная и структурированная. Изначально разрабатывалась как архитектура Информационных Систем. Основная идея заключается в том, чтобы обеспечить возможность последовательного описания каждого отдельного аспекта системы в координации со всеми остальными. Модель «Захмана» используется для описания предприятия в целом, так что предложенная модель, вообще говоря, может использоваться как средство для описания архитектур сложных производственных систем любого типа. Основные характеристики данной модели:

- целостность в отношении предприятия;
- обсуждений сложных вопросов с использованием относительно небольшого количества нетехнических понятий;
- применимость для решения задач, то есть возможность работать с абстракциями и сущностями, выделяя и изолируя отдельные параметры системы без потери восприятия предприятия как целого;
- простота описания

Модель Захмана имеет такие преимущества перед другими моделями:

- Отличается своей простотой понимания как техническими, так и нетехническими специалистами.
- Более детальными описаниями компонентов архитектуры
- Возможностью применения для планирования, позволяющего лучше принимать решения.
- Наиболее наглядным представлением компонентов компании.
- Описанием сложной архитектуры небольшим количеством нетехнических понятий.
- Независимостью конкретных инструментов описания.
- Может использоваться как средство для описания архитектур сложных производственных систем любого типа.

3 Матрица Захмана						
	МОТИВЫ	ЛЮДИ	ГРАФИКИ	ДАННЫЕ	ФУНКЦИИ	СЕТЬ
Потребности цели	Конкуренты Товары	Партнеры	События			
Бизнесмодель	Бизнесплан					
Логическая (системная) модель АС	Бизнес-правила					
Техническая архитектура ИС	Условия/действия					
Детальная реализация	TRIGGER ALARM	read string	on event t > t1 ...	CREATE TABLE	BEGIN BLOCK	C>PING
Практика использования		Умения			Меню	Wait, please

Архитектура Предприятия – матрица «Zahman Framework»

Архитектура Предприятия на основе методологии «FEAF»

FEAF- фреймворк разработанный правительством США, как некий подход для развития информационных технологий правительственных учреждений, приведенный к использованию единой архитектуры.

В основе FEAF лежат пять эталонных моделей:

- Исполнительная модель.
- Бизнес-модель.
- Сервисная модель Компонента.
- Техническая эталонная модель.
- Эталонная модель данных.

Одно из полезных свойств фреймворка FEA – принцип сегментного подхода, дает возможность ускорить внедрение «Архитектуры предприятия». Процесс разработки архитектуры предприятия по методологии FEA включает в себя следующие этапы:

- Анализ Архитектуры
- Архитектурное определение
- Стратегия инвестиций и финансирования
- План управления программой и реализация проекта

Архитектура Предприятия на основе методологии «GARTNER»

Методология Gartner – эту модель можно описать как набор рекомендаций по созданию архитектуры предприятия. Модель Gartner 2002 года сформулирована в виде четырех связанных, взаимозависимых и усложняющихся уровней:

- Среда бизнес-взаимодействия (Business Relationship Grid);
- Бизнес-процессы и стили бизнес-процессов;
- Шаблоны;
- Технологические строительные блоки (кирпичики – bricks).

Методология Gartner – по сути своей не является методологией, как например

структурированная модель Захмана, ни процессом как TOGAF, ни как FEA. Gartner – является набором практических рекомендаций. Данная методология является сборником советов по построению архитектуры предприятия от одной из наиболее известных в мире консалтинговых ИТ-компаний – Gartner.

Данный фреймворк представляет собой трехмерный куб, состоящий из слоев:

- Горизонтальные слои.
- Вертикальные домены.
- Вертикальные элементы технической архитектуры.

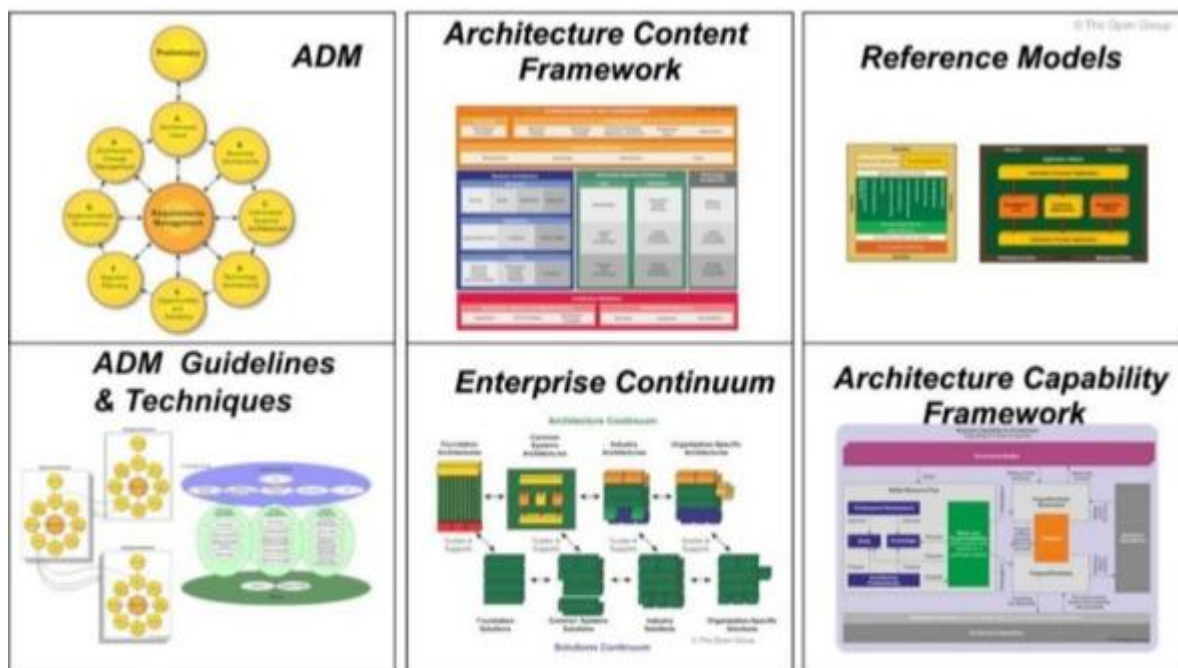
Архитектура Предприятия на основе методологии «TOGAF»

Основным полем для применения TOGAF является, прежде всего, программная инфраструктура информационной системы. Она в наилучшей мере подходит для описания интеграционных компонент, использующихся для поддержки широкого спектра корпоративных приложений, прежде всего, критичных для бизнеса. Описание модели:

- Обзор бизнес – архитектуры
- Описание существующей системы с необходимой степенью детализации
- Выявление и описание элементарных архитектурных блоков – кандидатов на использование в новой архитектуре
- Разработка черновика технического отчета
- Направление черновика отчета на рецензирование

TOGAF позиционируется не как некоторая эталонная модель, а как «средство для разработки архитектур информационных систем». Основное назначение – ускорить и облегчить процесс разработки архитектуры конкретной организации, обеспечивая при этом возможность будущего развития. Рассмотрим построение Архитектуры Предприятия на основе методологии «TOGAF» более детально, который на мой взгляд имеет ряд преимуществ:

- Подход TOGAF позволяет построить весь архитектурный процесс – от запуска практики до результатов.
- TOGAF – это де-факто является стандартом. Имеется программа сертификации по TOGAF.
- TOGAF – абсолютно бесплатен. Множество открытых ресурсов, скачивайте и используйте.
- TOGAF содержит полный набор инструментов для создания и развития архитектурной практики в организации. Есть пошаговый процесс для разработки описания Архитектуры Предприятия и полный набор инструментов, шаблонов и т. д.
- TOGAF совместим с другими Фреймворками, например, с «Zahman Framework». Как архитектурный процесс модель TOGAF дополняет модель Захмана – которая, классифицируется как архитектурная таксономия. Захман показывает, как следует классифицировать артефакты. Модель TOGAF описывает процесс создания артефактов.



Структура Архитектуры Предприятия «TOGAF»

Методология TOGAF и инфраструктура Захмана хоть и объединены к категории «инфраструктур предприятия», но имеют отличия в своих принципах, структурах и компетенциях. TOGAF- представляет собой функциональную и динамичную инфраструктуру, которая включает руководящие принципы моделей процесса их использования. В то время как фреймворк Захмана представляет собой статичную структуру архитектуры, наиболее эффективна для применения анализа и метаанализа фреймворков инфраструктур. Несмотря на значительные отличия данных фреймворков их можно использовать совместно.

Базовые принципы

Процесс создания конкретной архитектуры предприятия рассматривается как переход от общей архитектуры к специализированной. Методика разработки архитектуры в модели TOGAF представляет собой процесс осуществления такого перехода. В модели TOGAF наиболее обобщенные архитектуры называются фундаментальными архитектурами. Эти принципы построения архитектуры теоретически могут использоваться практически любой ИТ-организацией в мире.

Следующий уровень специализации в модели TOGAF называется общесистемными архитектурами. Эти принципы прослеживаются во многих – возможно, не во всех – типах предприятий. Далее идет отраслевой уровень архитектурой. Эти принципы характерны для предприятий, занятых в одной сфере деятельности. И наконец финальный уровень – это уровень архитектуры организации. Это самый высокий уровень специализации в модели TOGAF. Это архитектуры конкретных предприятий.

В состав модели TOGAF входят две основные компоненты:

- *методика ADM (Architecture Development Method)* , определяющая процесс разработки архитектуры.

- *Базовая Архитектура (Foundation Architecture)*. Она дополняется соответствующей базой данных ресурсов, включающей описания архитектурных принципов, примеров реализации, а также специализированный язык ADML.

Описание TOGAF включает в себя 7 частей:

- *Introduction*. Содержит высокоуровневое описание ключевых концепций

Архитектуры в целом и TOGAF в частности.

- *Architecture Development Method (ADM)* . Ключевая часть TOGAF, описывает пошаговую методику разработки Архитектуры Предприятия.

- *ADM Guidelines and Techniques* . Включает в себя описание правил и техник, которые используются в TOGAF ADM.

- *Architecture Content Framework* . Описывает подход к описанию Архитектуры Предприятия. Содержит метамодель архитектурных артефактов, структуру и описание типовых архитектурных артефактов.

- *Enterprise Continuum & Tools* . Описан подход к категоризации и хранению результатов архитектурных активностей.

- *TOGAF Reference Models* . Описание эталонных моделей, которые вы можете использовать в ваших проектах.

- *Architecture Capability Framework*. Подход к организации архитектурной практики в компании. Структура, процессы, роли, навыки и полномочия, требуемые для работы архитектурной практики в компании.

В качестве основных процессов построения Архитектуры Предприятия важно внедрить всего четыре ключевых процесса:

- Создания и развития Архитектуры Предприятия.
- Управления изменениями.
- Контроль реализации архитектурных решений.
- Управления практикой.

Метод Развития Архитектуры (Architecture Development Method ADM) TOGAF

В TOGAF процессы создания и развития, управления изменениями, контроля реализации архитектурных решений интегрированы в единый архитектурный цикл Метод Развития Архитектуры (Architecture Development Method ADM). Данный метод можно и нужно адаптировать под задачи вашей компании на всех уровнях разработки архитектуры. При этом, нет необходимости делать все возможные документы. Не нужно погружаться во все детали. На каждом этапе ADM предлагает готовый набор техник, инструментов, шаблонов и чек листов. Метод Развития Архитектуры (ADM) содержит десять фаз. Каждая фаза, в свою очередь разбивается на под-процессы (этапы), отдельные работы и так далее.

Например, фаза D включает следующие основные под-процессы:

- *Описание существующей технологической архитектуры.*
 - ° Обзор бизнес-архитектуры, архитектуры данных и приложений для определения начальных данных и необходимой степени детализации.
 - ° Описание существующей системы с необходимой степенью детализации, которая выбирается для того, чтобы можно было выявить необходимые изменения при формировании целевой архитектуры. Формирование реестра используемых платформ программного и аппаратного обеспечения.
 - ° Выявление и описание элементарных архитектурных блоков – кандидатов на использование в новой архитектуре. Фактически, речь идет о возможных архитектурных шаблонах.
 - ° Разработка черновика технического отчета, резюмирующего основные результаты изучения существующего состояния и возможности использования типовых блоков.
 - ° Направление черновика отчета на рецензирование, анализ комментариев и внесение, при необходимости, поправок.
- *Формирование целевой технологической архитектуры.*
 - ° Описание существующей системы в терминах TOGAF.
 - ° Определение перспектив (представлений) архитектуры.

- °Формирование модели целевой архитектуры.
- °Определение ИТ-служб (сервисов).
- °Подтверждение учета бизнес-требований.
- °Определение архитектуры и используемых блоков (шаблонов).
- °Проведение анализа расхождений (gap analysis).



Рисунок: «TOGAF» и Метод Развития Архитектуры (Architecture Development Method ADM).

Таблица: Фазы и задачи Метода Развития Архитектуры

Предварительная фаза. Основные задачи:

- Создать архитектурную практику,
- подготовить компанию к запуску архитектурных проектов,
- заручиться поддержкой руководства,
- сформулировать архитектурные принципы,
- адаптировать методологию под цели и задачи компании

Фаза А – Видение архитектуры. Основные задачи:

- Запустить архитектурный проект, определить цели и задачи, определить рамки, предположения и ограничения проекта, разработать видение архитектуры, определить всех заинтересованных лиц,
- разработать «Устав проекта» и получить формальное подтверждение старта проекта.

Фаза В – Бизнес Архитектура. Основные задачи:

- Разработать архитектуру с описанием текущей и целевой архитектуры,
- Анализ расхождений

Фаза С – Архитектура Информационных Систем. Задачи:

- Разработать архитектуру с описанием текущей и целевой архитектуры,
- Анализ расхождений

Фаза D – Техническая Архитектура. Основные задачи:

- Разработать архитектуру с описанием текущей и целевой архитектуры,

- Анализ расхождений

Фаза E – Возможности и решения. Основные задачи:

- Выполнить начальное планирование реализации задач проекта.

- Идентифицировать основные проекты внедрения и сгруппировать их в переходные архитектуры.

Фаза F – Планирование миграции. Основные задачи:

- Анализ затрат и рисков.

- Разработка детального плана внедрения и миграции.

Фаза G – Управление реализацией. Основные задачи:

- Архитектурный надзор за проектами внедрения.

- Подготовить архитектурные контракты.

- Обеспечить соответствие архитектуре результатов проектов внедрения.

Фаза H – Управление изменениями архитектуры. Задачи:

- Подготовиться к следующему витку жизненного цикла архитектуры.

- Процесс управления изменениями должен обеспечить соответствие архитектуры актуальным потребностям бизнеса и дать максимальную ценность бизнесу.

Управление требованиями. Основные задачи:

- На каждой фазе архитектурного проекта собираете и согласуете бизнес требования.

- Требования должны быть идентифицированы, сохранены, определены приоритеты и использованы на соответствующих фазах архитектурного проекта.

Спецификация TOGAF также позволяет гибко работать с этапами. В самой спецификации говорится следующее:

Перед применением методики разработки архитектуры необходимо проверить компоненты на применимость, а затем связать их с конкретными обстоятельствами отдельного предприятия. Это позволяет создать методику разработки архитектуры для конкретного предприятия.

Модель TOGAF позволяет выполнять этапы частично, пропускать их, объединять, изменять порядок и вносить изменения в соответствии с конкретными требованиями. Неудивительно, что два сертифицированных консультанта по TOGAF могут разработать два совершенно различных процесса – даже при работе с одной и той же организацией.

Модель TOGAF обладает еще большей гибкостью в отношении созданной архитектуры. Фактически TOGAF, как это ни удивительно, «ничего не знает» об архитектуре. Окончательная архитектура может с одинаковым успехом быть хорошей, плохой или неопределенного качества. В TOGAF описывается, как создать архитектуру предприятия, но не описывается, как создать хорошую архитектуру. Качество конечного продукта зависит от опыта персонала компании и консультанта по TOGAF. Те, кто внедряет TOGAF в надежде получить чудодейственное средство, будут жестоко разочарованы (впрочем, как и при использовании любой одной методологии).

Базовая Архитектура (Foundation Architecture)

Базовая Архитектура, включает в себя:

- набор наиболее общих служб и функций, объединенных в Техническую Эталонную Модель (Technical reference model – TRM);

- набор элементарных архитектурных элементов, которые используются как «строительные блоки» при построении конкретных решений;

- база данных стандартов (Standards Information Base).

Концепция использования Базовой архитектуры определяется в соответствии с иерархией архитектур, входящих в общий континуум определений. В TOGAF техническая

эталонная модель рекомендуется к использованию, но не является обязательной. В общем техническая эталонная модель, не лишена недостатков по следующей причине: она направлена на обеспечение переносимости приложений в ущерб их способности к взаимодействию и автономности. Для организаций модель TOGAF в значительной степени сводится к методике разработки архитектуры. В этом смысле компонента Базовой Архитектуры, содержащая набор служб и стандартов, является некоторой абстрактной реализацией ИТ-системы в целом. Архитектура Общих Систем реализуется путем выбора и интеграции определенных служб для формирования выделенных блоков, которые могут (возможно, повторно или в различных комбинациях) использоваться в различных функциональных областях, таких как архитектура безопасности, сетевая архитектура и т. п.

Следующая степень детализации реализуется на уровне Отраслевой Архитектуры, которая добавляет специфичные для каждой индустрии модели данных, приложения, стандарты, бизнес-правила, а также, при необходимости, процедуры взаимодействия различных отраслевых систем между собой. Наконец, на последнем уровне Архитектуры Организации формируется архитектура ИТ-систем конкретного предприятия, учитывающая все его особенности, в том числе наличие унаследованных систем, планы и возможности реализации, организацию данных на физическом уровне и т. п.

В состав Эталонной Модели, в свою очередь, входит система (таксономия) общих служб, включающая такие службы, как Обмен и преобразование данных, Управление данными, Поддержка интернационализации, Службы Каталогов и т. п.

Для всех используемых в архитектуре служб, наряду с функциональным назначением, необходимо определить и уровень качества реализации, то есть такие характеристики как управляемость, гибкость, гарантированность, удобство использования и т. п. При этом следует учитывать, что некоторые службы являются в этом плане взаимозависимыми. Например, для обеспечения заданного качества службы интернационализации могут потребоваться специализированные компоненты службы разработки программного обеспечения для создания и тестирования соответствующих программных продуктов.

Архитектурные принципы представляют собой как бы фундаментальные «аксиомы», которые используются в качестве «отправных точек» как для оценки существующей системы, так и для разработки отдельных архитектурных решений. Вообще говоря, архитектурные принципы являются подмножеством более общего понятия ИТ-принципов, которые определяют основные

аспекты всей деятельности, связанной с применением информационных технологий. ИТ-принципы, в свою очередь, являются детализацией еще «более общих» принципов, определяющих деятельность предприятия в целом.

В состав набора принципов могут входить обоснования для формирования системы требований или критериев оценки тех или иных решений. Например, такой принцип, как «минимизация числа поставщиков программного обеспечения», может быть в дальнейшем конкретизирован в зависимости от особенностей предприятия, как требование «единой СУБД для всех критичных для бизнеса приложений» или же как «использование той же СУБД, что и уже применяемая». Архитектурные принципы могут также использоваться для обоснования значимости самого понятия Архитектуры и необходимости ее разработки для бизнеса предприятия, а также для выбора вариантов реализации этого процесса.

Принципы являются взаимозависимыми и должны применяться в целостном наборе. «Хороший» набор принципов должен удовлетворять таким естественным критериям, как доступность для понимания, точность формулировок, полнота, последовательность и стабильность (не нужно путать с неизменяемостью!) Обычно число принципов не превышает 20, чтобы не ограничивать гибкость архитектуры или чтобы избежать чисто формального определения принципов, которые неработоспособны на практике.

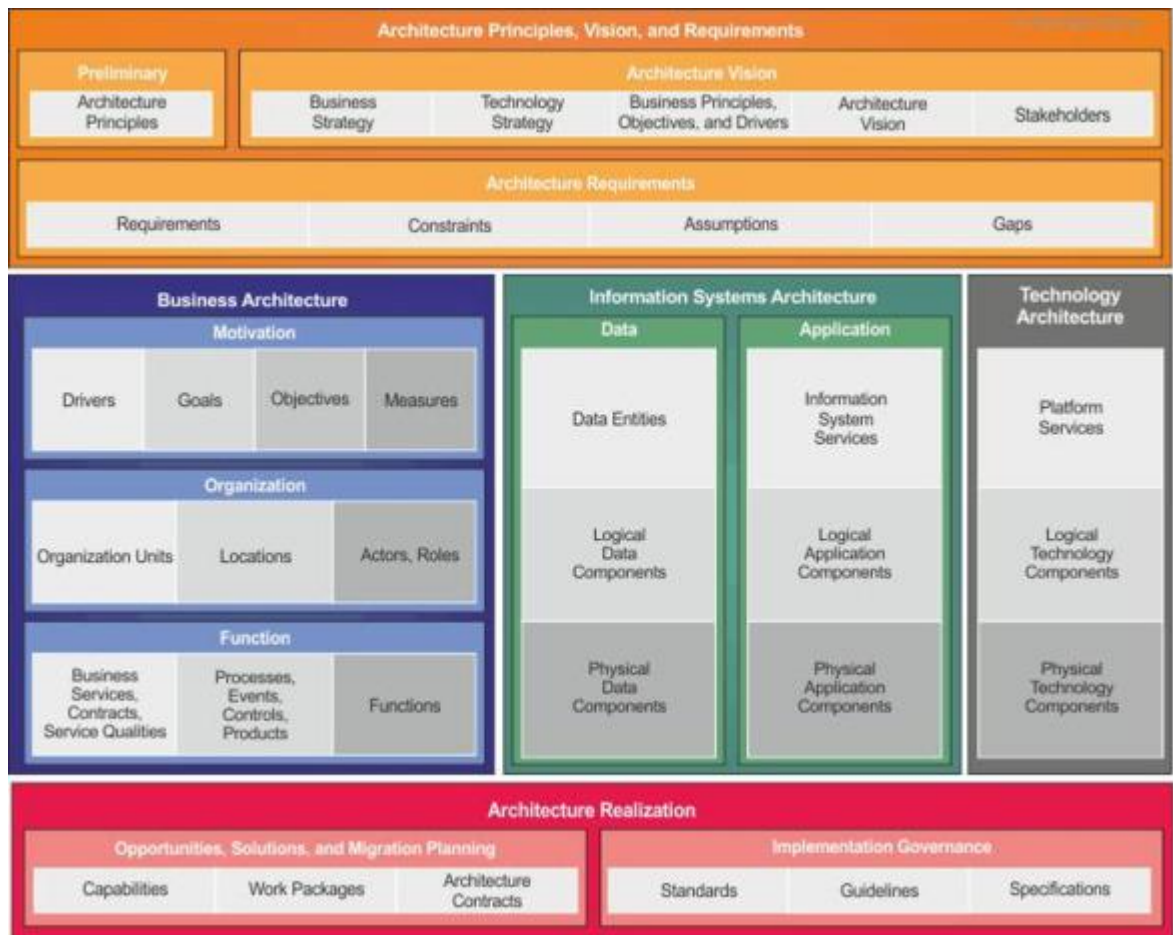


Рисунок: Архитектуры Предприятия «TOGAF»

Примеры принципов, используемых при создании архитектуры TOGAF (Название и содержание):

- *Пример использования* – Сформулированные принципы управления ИТ применимы для всех случаев и подразделений организации.
- *Максимальная польза* – Решения в области ИТ принимаются исходя из максимума пользы для организации в целом.
- *Привлечение всех* – Управление информацией есть дело каждого.
- *Непрерывность бизнеса* – Деятельность предприятия должна обеспечиваться, несмотря на возможные помехи в работе ИТ.
- *Общее использование* – Предпочтение должно отдаваться разработке или внедрению приложений, применимых в масштабах всего предприятия, а не отдельных его подразделений.
- *Соответствие законодательству* – Управление ИТ не должно противоречить применяемому законодательству и принятым регламентам, однако это не есть препятствие к улучшению бизнес-процессов, влекущему за собой изменение этих регламентов.
- *Ответственность ИТ-службы* – ИТ-служба является ответственным владельцем ИТ-ресурсов и исполнителем процессов для удовлетворения требований бизнеса.
- *Защита интеллектуальной собственности* – Обеспечение защиты интеллектуальной собственности организации должно быть реализовано на уровне архитектуры, процессов эксплуатации и управления ИТ.
- *Данные являются активом* – Данные в ИТ-системе предприятия имеют определенную ценность и должны соответственно управляться, быть общими и доступными для пользователей с учетом их прав доступа.
- *Обеспечение качества* – Каждый элемент данных должен иметь ответственного за качество.

•*Общие метаданные* – Метаданные должны быть едиными в рамках предприятия и доступными для всех пользователей.

•*Безопасность данных* – Данные должны быть защищены от неавторизованного использования и распространения.

•*Технологическая независимость* – Прикладное ПО не должно зависеть от специфичных моделей оборудования и системного ПО.

•*Простота использования* – Приложения позволяют сконцентрироваться на выполнении бизнес-задач за счет единого интерфейса, минимизации специфики работы, интеграции систем, снижения вероятности неправильного использования.

•*Обоснованность и своевременность изменений* – Изменения в информационной системе и приложениях производятся только в соответствии с запросами бизнеса, но в случае появления такой необходимости – в нужное время.

•*Взаимодействие* – Взаимодействие Компоненты программного и аппаратного обеспечения должны обеспечивать интеграцию между собой в соответствии с общими стандартами.

•*Минимизация разнообразия* – Уменьшение числа различных вариантов применяемых платформ, продуктов и версий.

Процесс Управления Архитектурной Практикой

Архитектурная практика представляет из себя практику внедрения архитектурного проекта в организации. Архитектурная практика состоит из четырех ключевых элементов:

•*Люди.* Они основа любой деятельности в компании. Если люди не знают, не умеют, не используют, не участвуют, не делают, не хотят, то все остальное бесполезно. Забыли про людей – забудьте про результаты.

•*Артефакты.* В процессе работы люди должны достигать заранее определенных результатов. Также они создают артефакты, которые позволяют обмениваться информацией, обсуждать задачи и проблемы, сохранять идеи для последующего воплощения, контролировать достижение результатов и т. д.

•*Процессы.* Для достижения результатов люди должны делать правильные действия в правильной последовательности. Все люди ошибаются, но если они следуют заранее определенным процессам, то вероятность ошибок снижается, а их последствия удастся быстро устранить. Процессы помогают превратить хорошие идеи в результаты. Так что от них никуда не уйдешь.

•*Управление.* Без правильного управления архитектурная практика обречена на провал. Требуется заранее определить рамки и правила практики, взяв за основу стандартные процессы, артефакты, роли и т. д. Придумывать правила по ходу игры очень опасно. Люди будут дезориентированы, процессы будут сбоить, результаты будут не те и не тогда, когда нужно.



Рисунок: Управление Архитектурной Практикой «TOGAF»

Процесс управления архитектурной практикой необходим для того, чтобы исключить обычные ошибки, совершаемые людьми в процессе работы над задачей или проектом. Люди чаще всего не достигают результатов, если:

- залезают в дебри теорий и исследований;
- выполняют бесполезную работу;
- долго готовятся к выполнению работы;
- изобретают велосипед;
- «оптимизируют» свою работу вместо её выполнения;
- излишне теоретизируют;
- ищут ответственных и виноватых;
- считают себя самыми умными;
- избегают неприятной работы.

Подход к управлению архитектурной практикой состоит из шести основных элементов:

- **Методология** — это основной элемент подхода. Он определяет процессы компании для разработки, обновления и реализации Архитектуры Предприятия. Роли и их обязанности.

- **Артефакты** — набор, шаблоны и правила заполнения документов, таблиц, схем, при помощи которых описана Архитектура Предприятия.

- **Стандарты** — это стандарты (законы, правила) ведения бизнеса и ИТ, которые использует компания в своей работе. Это могут быть международные стандарты, российские стандарты, стандарты отрасли, региона, компании.

- **Лучшие практики и готовые модели** — доказанные способы реализации решений, проверенные в вашей или в других компаниях.

- **Регламенты и правила** — документы, в которых описаны цели, задачи, организационная структура, правила работы и границы архитектурной практики. Правила работы с другими подразделениями. Полномочия архитекторов. Регламенты должны быть интегрированы с другими регламентами компании, особенно ИТ департамента.

- **Управленческие воздействия** со стороны менеджеров практики. Они направлены на то, чтобы компания получила практические результаты. Нужно планировать, заставить людей следовать процессам, стартовать архитектурные проекты, решать конфликты, контролировать промежуточные результаты и т. д. Все прочие элементы не будут работать без управления.

Порядок внедрения архитектурной практики. Во-первых, разработать все эти элементы для компании с нуля — это неподъемная задача. Поэтому для её решения нужно взять уже созданные методологии и адаптировать их к нуждам компании. Во-вторых, внедряйте их

постепенно, как часть развития практики. Внедрение каждого элемента должно давать ценность практике. В-третьих, соблюдайте баланс между бюрократией и личной инициативой. И последнее – экспериментируйте. Проверяйте новые подходы. Если они дают ценность, опишите их в регламенте и используйте в ваших следующих проектах.

Ключевые документы и шаблоны методологии TOGAF

Для внедрения методологии TOGAF возникает вопрос какой минимальный набор документов необходим для ведения архитектурного проекта? Лишние документы – лишние затраты времени и денег. По исходя из собственного опыта и теории (при подготовке к сертификации), минимальный «джентельменский набор» может состоять из восьми документов:

- *Основы методологии* (Templates, Business Principles, Goals, Drivers). Необходим для понимания миссии, цели, стратегию компании. Зафиксировать бизнес принципы. Шаблон «TOGAF 9 Templates, Business Principles, Goals, Drivers.doc»

- *Архитектурные принципы* (Architecture Principles) – это правила, которыми руководствуются в работе над архитектурой. На их основе принимают архитектурные решения. Принципы нужно сформулировать на основе примеров из TOGAF. Использование принципов при работе над архитектурой доказало свою эффективность. Шаблон – «TOGAF 9 Template Architecture Principles.doc»

- *Видение архитектуры* (Architecture Vision) – это высокоуровневое описание желательного конечного продукта архитектурного проекта. То есть это те результаты, которых нужно достичь. Описание решения тех проблем и задач, ради которых стартуют проект. Этот документ важен для взаимодействия со спонсором проекта и другими заинтересованными лицами. Шаблон – «TOGAF 9 Template Architecture Vision.doc»

- *Устав проекта* (Statement of Architecture Work) – соглашение между спонсором и проектной командой о выполнении работ. В него включают все рамки, ограничения, предположения, сроки, бюджет, правила проекта. В нем конкретно назначают менеджера проекта и прописывают его права и обязанности. Сюда же включают как приложение видение архитектуры как описание рамок проекта. Шаблон – «TOGAF 9 Template Statement of Architecture Work.doc»

- *Описание архитектуры* (Architecture Definition) – это представление текущей и целевой архитектуры. Он охватывает каждый из архитектурных доменов (бизнес, данные, приложения, технологии). А также анализ расхождений между текущим и будущим состоянием. Шаблон – «TOGAF 9 Template Architecture Definition.doc»

- *Спецификация требований к архитектуре* (Architecture Requirements Specification) – документ, в котором собраны все требования, ограничения, предположения, критерии достижения. Шаблон – «TOGAF 9 Template Architecture Requirements Specification.doc»

- *Переходная архитектура* (Transition Architecture) – Реализация целевой архитектуры проходит в несколько этапов. Каждое промежуточное состояние должно быть работоспособно и давать компании большую ценность. В этом документе сгруппированы проекты по каждому из таких этапов. Шаблон – «TOGAF 9 Template Transition Architecture.doc»

- *План реализации и миграции* (Implementation and Migration Plan) – это сводный план реализации проектов, направленных на достижение целевой архитектуры. В него также включают выгоды, рамки, сроки, стоимость, риски, контрольные точки проектов. Шаблон – «TOGAF 9 Template Implementation and Migration Plan.doc»

Такой набор документов можно сделать максимально быстро и без больших затрат. Если предполагается воспользоваться услугами третьих сторон, то рекомендую включить ещё один документ – архитектурный контракт. Это соглашение между архитекторами и исполнителями ИТ проекта. Шаблон – «TOGAF 9 Template – Architecture Contract.doc» При

приемке проекта вам будет легче получить нужный результат, если вы о нем заранее договорились.

Стратегия Управления

При формировании ИТ Стратегии можно определить стратегию по вопросам «Технической Архитектуры» и «Архитектура Информационных Систем (сервисов)» ряда компонентов ИТ инфраструктуры, а также рекомендации по выбору того или иного решения.

Стратегия финансового контроля

Стратегия финансирования может предполагать поведение организации в вопросах финансирования ИТ. В частности, желательно иметь финансовую стратегию по таким вопросам как:

- При выборе решения по ИТ проекту, как приоритет руководствоваться стоимостью решения, даже если это идет в ущерб функциональности. Возможности решения должны соответствовать требованиям бизнеса с минимальной стоимостью.

- Ориентироваться на использование свободно распространяемого программного обеспечения

- Выравнивание по стоимости или функционалу.

Например, стоимость аренды каналов связи для разных филиалов банка может отличаться в зависимости от расстояния или географического расположения. Предположим, что стоимость 10 Mbps канала (стандартные и достаточные ИТ требования) для регионального филиала обходится 500 долларов. За ту же стоимость городской филиал может получить скорость канала до 100 Mbps. На текущий момент у этого филиала стандартная скорость 10 Mbps, но обходится за 100 долларов в месяц. Средняя стоимость канала связи для всех филиалов порядка 250 долларов. Руководство должно иметь определённую стратегию по данному вопросу: предоставить возможность филиалам наращивать скорость в пределах средней стоимости, максимальной стоимости или выравнивание всех по установленной скорости канала (10 Mbps).

Использование по возможности, ресурсы аутсорсинга при внедрении и сопровождении Информационных Систем и проектов или наращивать возможности и потенциал сотрудников ИТ департамента.

Стратегия административных регуляторов

Стратегия изменений может предполагать поведение организации в вопросах реакции на изменения требований и т.п. Как пример рассмотрим ситуацию, когда количество сотрудников остается неизменным, но скорость доступа в интернет значительно упала по причине активного использования. Как решение можно пойти по пути увеличения скорости канала и соответственно увеличением расходов. И так с определённой периодичностью данный вопрос будет возникать пока не дойдет до критической точки. Можно выбрать альтернативный «репрессивный» метод. ИТ департамент проведя анализ сетевого трафика определил, что вырос процент нецелевого использования интернета. Проведя ряд показательных казней руководство компании может добиться улучшения скорости использования интернета без увеличения стоимости используя административные рычаги управления.

Стратегия построения инфраструктуры

Стратегия выбора архитектуры

В качестве архитектуры решения могут быть рассмотрены следующие решения:

- Собственная инфраструктура (on premise)

- Облачная инфраструктура
- Гибридная архитектура

«On-premise» – ИТ активы физически располагаются на территории организации.

Преимущества:

•ИТ инфраструктура располагается на территории организации и контролируются ИТ сотрудниками организации.

- Относительно низкой стоимостью сопровождения (ОРЕХ) ИТ инфраструктуры.
- Автономность решений и более высокий уровень безопасности

Недостатки:

•Относительно высокие первоначальные вложения (CAPEX) в ИТ инфраструктуру.
 •Внедрение новых сервисов, или резкие скачки (роста) имеющихся сервисов трудно поддается планированию.

•Необходимость иметь в составе ИТ специалистов по поддержанию инфраструктуры (ремонт и обслуживание физических серверов, сетевого оборудования и т п). Все это ведет к дополнительным расходам.

- Косвенные расходы на инженерные системы ИТ инфраструктуры.

«Cloud based» – ИТ активы располагаются в «облаке».

Преимущества:

- Относительно низкие первоначальные вложения (CAPEX) в ИТ инфраструктуру.
- Высокий уровень планирования расходов на сопровождение ИТ инфраструктуры.
- Хорошая связь, линейная зависимость используемых ресурсов и их стоимости.
- Простота внедрения новых решений и расширения имеющихся ИТ сервисов.
- Нет необходимости в дополнительных сотрудниках.
- Нет необходимости в косвенных расходах на системы инженерные.

Недостатки:

- Относительно высокая стоимость сопровождения (ОРЕХ) ИТ инфраструктуры.
- Более высокие требования к каналам связи интернета и наличию резервных каналов.

«Hybrid» – комбинированное решения. Используются преимущества двух первых решений.

Преимущества: Использует достоинства обоих решений.

Недостатки: Более высокая стоимость внедрения (CAPEX) и сопровождения (ОРЕХ)

Рекомендации по выбору:

Для начальных проектов, небольших организаций, организаций с развитой географией и т п предпочтительно использование «Cloud based» решения. Для крепкой организации, финансовых институтов, организаций где выход в интернет не является требованием бизнеса и т п предпочтительно использование «On-premises» решения. «Hybrid» решения могут как дополнять ИТ инфраструктуру, так и заменять часть компонентов ИТ архитектуры.

Стратегия выбора платформа инфраструктуры

Если в качестве архитектуры развертывания выбрана собственная инфраструктура «On-premises», то возможны следующие варианты:

- Физические сервера как основа
- Платформа виртуализации как основа
- Смешанная инфраструктура, преобладание не наблюдается

«Физические сервера» – ИТ сервисы располагаются на физических серверах.

Преимущества:

•Относительно низкой стоимостью внедрения (CAPEX) ИТ сервисов для малых решений.
 •Ресурсы физического сервера полностью выделены по задачи конкретного сервиса.

Недостатки:

- Сложность сопровождения, с ростом инфраструктуры.
- Скорость развёртывания и восстановления.
- Не оптимальное использование вычислительных ресурсов.

«Платформа виртуализации» – ИТ сервисы располагаются на платформе виртуализации в виде виртуальных машин.

Преимущества:

- Относительно низкая стоимость сопровождения (OPEX) в ИТ инфраструктуру.
- Фактически является «де-факто» стандартов развертывания «On-premises» решений.

Недостатки: Относительно высокая стоимость внедрения (CAPEX) ИТ инфраструктуры.

Рекомендации по выбору:

Для небольших, отдельно стоящих или удаленных ИТ сервисов, или же высоконагруженных систем предпочтительно использование «физических серверов» решения. Для всех прочих случаев, использование платформы виртуализации предпочтительнее.

Стратегия выбора Системы Хранения Данных

Если в качестве архитектуры развертывания выбрана собственная инфраструктура «On-premises», то возможны следующие варианты:

- Физические сервера и (DAS)
- Централизованная Система Хранения Данных (NAS, SAN)
- Распределённая Система Хранения Данных (DDS, SDS)

«Физические сервера» – данные располагаются на физических серверах.

Преимущества:

•Относительно низкой стоимостью внедрения (CAPEX) ИТ сервисов для малых решений.

- Ресурсы физического сервера полностью выделены по задачи конкретного сервиса.

Недостатки:

- Сложность сопровождения, с ростом инфраструктуры.
- Скорость развёртывания и восстановления.
- Не оптимальное использование вычислительных ресурсов.

«Централизованная Система Хранения Данных (NAS, SAN)» – Данные располагаются на частично или полностью единой СХД. СХД представляет из себя единый комплекс состоящий из контролеров, и полок размещения дисков.

Преимущества: Относительно низкая стоимость сопровождения (OPEX) в ИТ инфраструктуру.

Недостатки: Относительно высокая стоимость внедрения (CAPEX) ИТ инфраструктуры.

«Распределённая Система Хранения Данных (DDS, SDS)» – Данные распределены между различными физическими серверами. СХД представляет из себя комплекс, распределённый в сети и состоящий из контролеров данных и дисковых хранилищ.

Рекомендации по выбору:

Для небольших, отдельно стоящих или удаленных ИТ сервисов, или же высоконагруженных систем предпочтительно использование «физических серверов» решения. Для всех прочих случаев, использование платформы виртуализации предпочтительнее.

Стратегия выбора производителя

Стратегия выбора программного и аппаратного обеспечения определяет подход к выбору производителя, стандартизации и т. п. В качестве вариантов, могут быть рассмотрены следующие варианты:

- Использование ограниченного списка производителей
- Использование произвольного списка производителей

Использование определённого производителя для каждой категории ИТ активов. Использование стандартов аппаратного и программного обеспечения в организации.

Преимущества:

•Внедрение стандартов ИТ активов упрощает процесс обеспечения сотрудников организации ИТ активами.

- Облегчает внедрение и сопровождение ИТ инфраструктуры
- Повышает уровень информационной безопасности организации.

Недостатки: Относительно высокая стоимость и зависимость от производителя и/или поставщика.

Использование произвольного производителя. Использование рекомендаций вместо стандартов для аппаратного и программного обеспечения в организации.

Преимущества: Относительно низкая стоимость и быстрота приобретения ИТ активов.

Недостатки:

- Процесс обеспечения сотрудников организации ИТ активами сложный и более долгий.
- Усложняет внедрение и сопровождение ИТ инфраструктуры
- Снижает уровень информационной безопасности организации.

Рекомендации по выбору:

Для организаций имеющих тесную интеграцию и зависимость бизнеса и Информационных Технологий или большую численность сотрудников рекомендуется использование первого варианта лицензирования.

Стратегия лицензирования

Стратегия лицензирования определяет подход к методам лицензирования. В качестве вариантов, могут быть рассмотрены следующие варианты:

Использование лицензионного соглашения уровня «Предприятия» с ежегодным продлением возможности обновления программного обеспечения. Лицензирование является непрерывным процессом в ИТ.

Преимущества:

•Большая степень свободы в вопросах лицензирования.

•Поддержка ИТ инфраструктуры и информационной безопасности на высоком уровне за счет использования более современных версий систем и решений.

•Обновление систем происходит плавно, без всплесков требований в ИТ ресурсах, людях и времени

Недостатки: Относительно высокая стоимость.

Покупка «коробочных» лицензий без продления обновления программного обеспечения. Лицензирование «по требованию».

Преимущества: Относительно дешевле по стоимости

Недостатки:

•Меньшая степень свободы в вопросах лицензирования.

•Поддержка ИТ инфраструктуры и информационной безопасности снижается по причине использования не самых современных версий систем и решений.

•Обновление систем происходит скачками (раз в три, четыре года), и требует наличие дополнительных ИТ ресурсов, людей и времени.

Рекомендации по выбору:

Для организаций имеющих тесную интеграцию и зависимость бизнеса и Информационных Технологий рекомендуется использование первого варианта лицензирования.

Стратегия построения инженерных систем

Для «On premise» и «Hybrid» решений требуется определиться с требованиями к инженерным системам.

К требованиям по инженерным системам можно отнести:

- Физические требования к помещению дата центра, серверной комнаты, коммуникационных шкафов и т.п.
- Требования к Структурированной Кабельной Системе.
- Требования по избыточности, резервированию и т.п.

Стратегия тестирования

Тестирование один из важных элементов при построении ИТ архитектуры. Уже на этапе проектирования ИТ архитектуры требуется определить вопросы по тестированию. Различают следующие площадки:

«**Test или Development**» – площадка с развернутыми отдельными ИТ сервисами. Используется для разработки сервисов или отладка элементов ИТ сервиса.

«**Pre-production**» – уменьшенная копия «**Production**» площадки со всеми компонентами ИТ архитектуры. Используется для отработки взаимодействия ИТ сервисов между собой. Так же позволяет эмулировать ситуации при поиске неисправностей, расчет производительности и т.п.

«**Production**» – площадка с развернутым вычислительными ресурсами предоставляющие ИТ сервисы.

Рекомендации по выбору:

В зависимости от предъявляемых требований со стороны бизнеса и финансовых возможностей организации возможны различные решения. Детальное описание рассмотрено далее в данном руководстве.

Стратегия уровня избыточности

Определение уровня избыточности компонентов ИТ инфраструктуры указывает требования к дублированию компонентов. Может рассматриваться на уровне:

•**Компонентов инженерных систем** (каналы и кабели связи, коммутационные стойки и т.п.). Резервирование (дублирование или избыточность) на уровне критически важных элементов, таких как:

- Каналы и кабели связи* (два и более проходящие по разным шахтам),
- Избыточное количество рабочих точек* (обеспечивает рост организации и резерв на отказ)

•**Компонентов устройства** (сервера, коммутатора и т.п.). Резервирование (дублирование) на уровне критически важных элементов устройства, таких как:

- Процессоры* (два и более процессоров),
- память* (две и более «банки» памяти),
- жесткие диски* (два диска в RAID1 массиве + один резервный)
- сетевые карты и адаптеры* (две карты с одним и более портами)
- блоки питания* (N+N или N+1)
- Компонентов ИТ сервиса.** Резервирование на уровне устройств и типу их включения. Как пример:
 - Два сервера в отказоустойчивом кластере*

- *Два сервера выполняющих одну и ту же роль* (два контролера домена)
- *Два сервера выполняющих разные роли в штатном режиме, но могут принять роли соседа в случае отказа* (Файловый сервер и сервер печати. В случае отказа можно установить роль на соседний сервер).

• **Географически разнесенные устройства в пределах сайта.** Расположение пары устройств в разных стойках, помещениях или зданиях в пределах одного сайта.

• **Географически разнесенные устройства на уровне сайтов.** Расположение пары устройств на разных сайтах.

Определение уровня резервирования зависит от критичности бизнеса к отказу или простою. Анализируется в процессе Управления Рисками, формализуется в документах по стандартам оборудования.

Стратегия по системам резервирования и архивирования

К системам резервирования и архивирования ИТ инфраструктуры можно определить следующие требования:

- Компоненты систем должны быть установлены на выделенных физических элементах (серверах, СХД и т.п.)

- Возможно совмещение систем резервирования и архивирования на одних компонентах.

- Права доступов для учетных записей (автоматического) резервного копирования по возможности не должны предоставлять возможность удаления данных или же их перезапись.

Стратегия построения резервного сайта

Наличие компонента резервного сайта, один из важных элементов при построении ИТ архитектуры. Он имеет отношение к концепции информационной безопасности, отказоустойчивости и восстановления. Различают следующие виды отказоустойчивости:

- Отказоустойчивость на уровне избыточности компонентов
- Отказоустойчивость на уровне дублирования элементов
- Отказоустойчивость в пределах сайта
- Отказоустойчивость с географически распределённым сайтом

Подходы по внедрению Архитектуры Предприятия

При разработке архитектуры вашей компании необязательно начинать с разработки стратегической архитектуры. Безусловно, **подход «Сверху – Вниз»** (Стратегическая архитектура – > Архитектура сегмента – > Архитектура решений) самый распространенный и имеет множество преимуществ:

- Будет понятен общий вектор развития организации.
- На уровне сегментов и решений будет меньше разброда и шатаний.
- Общие правила и подходы на уровне организации, а затем их трансляция на уровень сегментов и решений.

- Общие для компании информационные системы и сервисы, повторно используемые на уровне сегментов и решений.

Основная идея движение **от «общего к конкретному»** (Generic- to – specific), а также непрерывное совершенствование ИТ архитектуры на основе требований бизнеса. Но вы можете использовать и другие подходы:

«Снизу – Вверх» (Архитектура решений – > Архитектура сегмента – > Стратегическая архитектура). От архитектуры конкретных проектных решений к стратегической архитектуре. Компания начинает с архитектуры решения. До старта проекта решение прорабатывается и описывается. Затем – более высокие уровни

Архитектуры Предприятия. Этот метод позволяет быстро получить ценность от методов Архитектуры Предприятия. Но есть вероятность, что без стратегической архитектуры, как основы, архитектуры различных решений «разъедутся». Придется потратить время и ресурсы на приведение их к общему знаменателю.

«От Сегмента» (Архитектура Сегмента – > Архитектура решений и стратегическая архитектура) Когда компании важно решить проблемы в конкретном подразделении, запустить новое направление бизнеса, либо если компания не готова к крупномасштабным внедрениям Архитектуры Предприятия и хочет «потренироваться на кошечках». Обкатать идеи на одном подразделении или направлении бизнеса. В зависимости от целей и сроков их достижения вам нужно выбрать подход для вашей компании.

Информационные системы вашей компании возможно далеки от идеала. Но выбросить их и переделать будет стоить очень дорого и займет много времени. Ценность такой инициативы сильно ниже нуля. Опытный архитектор «полечит» проблемы с интеграцией, информационной безопасностью, инфраструктурой, заплатками, а саму систему заставит давать большую ценность вашей компании. Реализация будет идти небольшими, точно выверенными доработками. Он будет решать конкретные проблемы, а не «делать все по уму». Замена системы – это серьезное изменение для компании, и для него должны быть веские аргументы.

Следующий важный вопрос при внедрении проекта построения Архитектуры Предприятия: Стоит ли привлекать консультантов или делать все самим (MAKE or BUY)? Однозначного ответа на него нет. Все зависит от конкретной организации, целей и возможностей. Для примера, представим ситуацию:

Мы заключаем контракт с уважаемой компанией «СУПЕР ПУПЕР КОНСУЛЬТАНТЫ и Ко». Через несколько месяцев получаем набор документов под названием «Архитектура компании БАНАНАС и Ко», в котором расписана правильная система, множество схем, описаний и т. п. Так сказать решение «под ключ». Заманчиво? Да скорее всего дорого, но быстро, профессионально, не один «комар» (читаем «аудитор») носу не подточит. Возможно.

Конечно, использование внешних ресурсов, чужого опыта и знаний – это один из самых быстрых способов достижения результатов. Но есть несколько минусов:

- План перехода будет подозрительно похож на список товаров и услуг этой уважаемой компании. Любой внешний исполнитель в рамках проекта будет продавать другие свои товары и услуги. Это общая практика и один из главных законов продаж.

- Вы получите только набор документов, а не архитектурную практику. У вас останется только описание. Процессы, люди и управление уйдут вместе с консультантами.

- Ваши люди так и не понюхают порошу, консультанты сделают всю работу. А опыт и знания будут использовать у нового заказчика. Ваши специалисты будут архитекторами только на бумаге. У них не будет ключевого навыка – умения принимать технические решения.

На мой взгляд, чтобы выстроить процессы в организации, нужны сильные и грамотные менеджеры, знакомый с культурой компании, имеющие теоретические и практические навыки, умеющие и заинтересованные в передаче опыта и знания коллегам и сотрудникам. Они должны играть главную роль и являться движущей силой организации.

Я бы рекомендовал привлечение внешних консультантов, но не отдавал бы архитектурную работу внешним исполнителям на 100%. В компании должны оставаться не только результаты проектов, но и люди, знания и опыт. Поэтому большую часть работы должны выполнять сотрудники вашей организации. Но под присмотром эксперта и с его помощью. Обязательно в проект внедрения должны быть включены ресурсы по обучению сотрудников. Как гласит народная мудрость «практика без теории слепа, теория без практики мертва».

Инструменты внедрения Архитектуры Предприятия

Как и какие выбрать инструменты для разработки Архитектуры Предприятия. На рынке представлены десятки инструментов. От бесплатных до дорогих. Внедрение некоторых из них может стоить сотни тысяч долларов. Я рекомендую использовать по возможности бесплатные или дешевые инструменты (если не имеются в наличии) по следующим причинам:

- На старте архитектурной практике ещё предстоит доказать свою эффективность, поэтому значительные инвестиции и упущенное время будут серьезным препятствием на пути ее создания.

- На начальном этапе лучше использовать простые и знакомые инструменты, не требующие дополнительного внедрения и обучения. Скорость внедрения определяет успех.

- Нужно наработать опыт и получить первые результаты, чтобы сформировать адекватные требования к дорогой системе.

- Только после того, как практика запущена, получены опыт и первые результаты, время переходить на специализированные продукты.

Какие минимальные требования к инструментам? Что они должны помогать вам делать?

- Писать и редактировать тексты, составлять схемы, вести таблицы, делать презентации и т. д.

- Размещать их на общедоступном ресурсе, регулировать права доступа к информации, обсуждать эти материалы.

Набор инструментов:

- Для составления документов, схем, таблиц и презентаций можно использовать стандартный офисный пакет, например, MS Office. Для него есть готовые шаблоны для документов. Есть расширения для Visio, при помощи которых можно нарисовать все нужные схемы.

- Для совместной работы можно использовать корпоративный портал, систему управления документами, корпоративную почтовую систему, корпоративную систему передачи сообщений или выделенный файловый ресурс в корпоративной сети организации. Выбор решения будет зависеть от того, что уже есть у вашей компании.

Рекомендации по внедрению

На основе требований и ограничений, определённых выше, можно суммировать основной подход при построении ИТ архитектуры компании:

- Сервис ориентированный подход к построению ИТ архитектуры
- Минимизировать риски за счет использования проверенных и хорошо зарекомендовавших себя технологий, и решений

- Снижение расходов за счет максимального и оптимального использования текущих ИТ активов и решений

- Снижение сложности и разнородности имеющейся инфраструктуры
- Максимально возможный рациональный подход к консолидации ИТ активов (железо, программное обеспечение), оставляя на периферии уровень поддержки пользователей и/или специализированных систем

- Множественное использование ИТ активов (ИТ персонал) на проектах внутри компании

- Стандартизация ИТ активов (железо, программное обеспечение и решения) для снижения стоимости владения, сложности сопровождения и повышения информационной

безопасности

- Введение единых ИТ политик и процедур в компании для снижения стоимости владения, сложности сопровождения и повышения информационной безопасности
- Автоматизация рутинных ИТ процессов для снижения стоимости владения, сложности сопровождения и повышения информационной безопасности
- Формирование единой политики информационной безопасности в организации
- Формирование проектной команды с высоким уровнем компетенции

Совместимость

Везде где это возможно, необходимо учитывать наличие имеющихся систем и по возможности максимально использовать выгоды данных систем. Это позволит снизить издержки на замену, или внедрению и сопровождению новых систем.

Следование основным принципам

При внедрении новых или промежуточных решений, или же при разворачивании бизнеса (или его расширении), рекомендуется руководствоваться основными требованиями, изложенными в данном документе. Стоимость решения и сопровождения ИТ инфраструктуры на прямую зависит от выбора того или иного решения.

Заключение

В заключение можно сказать, что построение Архитектуры Предприятия один из важнейших аспектов построения эффективного механизма корпоративного управления с интеграцией информационных технологий для получения наилучших результатов. Интегрирование механизмов Управления ИТ сервисами (ITSM), систему Управления Проектами (РММ) методов аудита и контроля (COBIT) позволит бизнесу добиться исключительных результатов и максимальной отдачи от ИТ.

Концепция Управления Проектами

Общие Положения

Управление проектом рассматривается как метод и набор процедур, основанных на принятых принципах управления, которые используются для планирования, оценки и контроля рабочих заданий, с целью получить желаемый конечный результат в установленные сроки, в рамках выделенных средств и в соответствии с требованиями к проекту. Данный раздел содержит основные принципы управления проектами, которые должны быть приняты во внимание при построении ИТ Архитектуры Предприятия. Любые проекты, в которые вовлечены ИТ (влияют на ИТ или зависят от ИТ), рассматриваются как ИТ проекты. В процессе планирования, разработки и внедрения различных сервисов ИТ архитектуры необходимо руководствоваться принципами «проектного» подхода.

Управление Проектами очень обширная тема, затрагивающие и тесно переплетающаяся с различными направлениями деятельности, такими как управление качеством, рисками, финансами и т. п. В данной главе мы кратко рассмотрим основные аспекты, методы и техники управления проектами.

Проект – это одноразовая, не повторяющаяся деятельность или совокупность действий, за определенное время, направленная на создание уникальных продуктов, услуг, результатов или четко поставленных целей. Признаки проекта:

- *Есть конкретная дата начала.* Ключевой признак проекта «временная составляющая», т. е. есть начало и конец проекта.
- *Есть конкретная дата конца.* Дата установить предполагаемый срок окончания

проекта, но зафиксировать условие окончания проекта по получению конечного результата или достижения целей проекта.

- *Результат проекта уникален.* Это второе отличие проекта от процесса или регулярной деятельности. «Уникальный» не означает абсолютно новый для всех, он может быть уникальным для организатора или команды.

- *Ресурсы и бюджет – ограничены.*

- *Специфический порядок выполнения заданий.* Он может предполагать временное изменения в иерархии подчинения и управления от установленного в организации.

Программа – отличается от проекта тем, что она больше по масштабу и может состоять из множества проектов. Так, например, у организации есть программа перехода к централизованной системе управления ИТ, которая может включать в себя несколько отдельных проектов.

Задача или набор рабочих заданий – представляет из себя набор действий, которые могут быть выполнены одним или несколькими лицами с помощью простого списка, задающего последовательность действий.

Ключевые аспекты Управления Проектами

Тройственная ограниченность или Треугольник проекта – описывает баланс между *содержанием* (объем работ или scope), *стоимостью* (cost) и *временем* (time, schedule) проекта, что влияет на конечный результат – *качество* (quality). Качество – это четвертый элемент проектного треугольника, который находится в центре, и любое изменение сторон влияет на него.

Как говорится в популярном слогане «Сделаем хорошо, быстро, дешево. Нужно подчеркнуть».

Вывод данного постулата сводится к одному: невозможно изменить один из факторов (деньги, перечень работ, время или качество) не повлияв по крайней мере на один из других факторов. Как пример:

- Чтобы приблизить дату окончания (время) проекта, вы можете потратить больше ресурсов (деньги) или убрать некоторые задачи (область охвата) из проекта.

- Чтобы сделать проект в рамках бюджета (деньги), вы можете либо сократить некоторые задачи (область охвата), что повлияет на возможности продукта (качество).

- Чтобы добавить в продукт новые возможности (качество), вы можете продлить срок проекта, чтобы выделить время на новые задачи (время), тем самым добавив новые задачи (область охвата) и привлечь новых людей, чтобы работать быстрее (затраты).

Идея всех методик и подходов сводится к фокусированию внимания на одном или нескольких факторах с контролем воздействия на оставшиеся.

Критерии успешности проекта – чтобы проект считался успешным фактические показатели, должны совпадать с запланированными в плане завершения проекта в срок, в рамках установленного бюджета и в соответствии с требованиями, предъявляемыми к конечному результату. Эти требования могут и должны быть сформулированы и включать в себя измеряемые критерии – показатели успеха проекта.

Цель руководителя проекта – достижения критериев успешности проекта.

Основная задача руководителя проекта – соблюдение баланса треугольника проекта.

Как показывает практика лишь четверть всех проектов достигает критериев успеха. Поэтому при планировании проекта желательно указывать основные факторы успеха проекта (например, бюджет проекта и неизменность результата), а также возможные допуски – разрешенные отклонения связанных факторов (например, превышение срока реализации проекта, но не более чем на десять процентов и т.п.).

Для удобства управления проектами, в организации можно ввести классификацию

проектов по различным категориям. Категории и признаки проекта каждая организация определяет самостоятельно. Как пример общей **классификации проекта по сложности**:

- Простой* — Проект, целью которого являются новые или улучшение существующих бизнес процессов, информационных систем, программного обеспечения, документов, сервисов, машин, оборудования. Будет изменяться или создаваться только один бизнес-процесс только в одном подразделении компании. Характеризуется как правило малой стоимостью проекта, небольшим охватом работ, коротким сроком и вовлечением не большого количества сотрудников.

- Сложный* — Проект, целью которого являются новые или улучшение существующих бизнес процессов, информационных систем, программного обеспечения, документов, сервисов, машин, оборудования. Будут изменяться или создаваться несколько бизнес-процессов или задействовано несколько подразделений компании. Характеризуется как правило высокой стоимостью проекта, большим перечнем задач, продолжительным сроком и вовлечением большого количества сотрудников.

Классификация по приоритету, позволяет определить порядок выполнения проектов: Низкий, Средний или Высокий. Проекты могут быть классифицированы по назначению в контексте взаимодействия с ИТ:

- Административные проекты* — связаны с изменениями в организации как правило не влияющие на состояние ИТ инфраструктуры, или без привлечения ИТ ресурсов.

- Внутренние проекты* — происходящие, как правило, внутри одного подразделения организации и характеризуются незначительными изменениями в ИТ инфраструктуре или с незначительным привлечением ИТ ресурсов

- ИТ проекты* — проекты, происходящие внутри организации, в значительной степени влияющие на состояние ИТ инфраструктуры, имеющие цель изменить ИТ инфраструктуру организации, или с привлечением значительных ИТ ресурсов организации.

Самая первая фаза (этап) проекта, вне зависимости от выбранного метода управления проектом, является **начальная стадия** или инициализация проекта. На этом этапе принимается решение по старту проекта. В контексте данной книги, инициаторами проекта могут выступать одна из двух сторон организации:

- Бизнес подразделения
- ИТ департамент.

Вводной информацией на данном этапе может служить стратегия организации или бизнес план.

Бизнес план — это документ, дающий развернутое обоснование проекта и возможность всесторонне оценить эффективность принятых решений, планируемых мероприятий, ответить на вопрос, стоит ли вкладывать деньги в данный проект.

Определение целей проекта — является одним из важнейших аспектов процесса управления проектом. Каждый проект должен иметь хотя бы одну основную цель и возможно несколько частных, вспомогательных целей. Цель имеет следующие функции:

- Задаёт направление работ по реализации проекта.
- Определяет конечные результаты в терминах конечных продуктов или услуг.
- Служить в качестве источника информации для разрешения спорных вопросов, касающихся проекта.

Формулировка основной цели должна быть ориентирована на действия, быть краткой и простой, а также как можно более понятной. Важно помнить, что цель должна быть сформулирована с использованием таких терминов, которые не вызовут непонимание у тех, кто будет участвовать в проекте, принимать решения или читать документы по проекту. На начальном этапе формулировка целей может быть размыта и выражать общее направление.

Определение заинтересованных сторон (Stakeholders) – позволяет определить, кто является непосредственным заказчиком, имеет права принятия окончательного решения и т. п. Кроме этого выявляются общие вопросы по организации проекта, такие как организация, состав рабочей группы по направлениям (на уровне руководителей), порядок взаимодействия, принятия решений, механизмы коммуникации и т. п.

Выходом данной фазы проекта является определение заинтересованных сторон, постановка целей проекта и общие вопросы организации. В зависимости от выбранной методики управления проектом могут быть сформированы дополнительные выводы и результаты. В качестве первичных документов начального этапа можно рассматривать бизнес план, устав проекта или протокол собрания.

Следующим этапом управления проектом может быть **этап планирования**. Планирование является наиболее важным и сложным этапом управления проектами. На данном этапе происходит основная работа, по детальной проработке проекта и формируется ответ на главный вопрос: готова ли организация к выполнению проекта и будет ли проект успешен. Уровень сложности зависит от выбранной методологии и сложности проекта. На данном этапе может быть собраны бизнес требования, конкретизация целей, определение критериев успешности, детализация задач, планирование ресурсов, времени и т. п. Основные документы на выходе этапа планирования могут представлять из себя план проекта, техническое задание и т. п.

Согласование и утверждение проекта – Данный этап или более верное определение «веха» или контрольная точка проекта, характеризуется ответом на главный вопрос: начинаем проект или нет. После положительного ответа руководства, проект переходит на стадию исполнения. Для различных методологий управления проектами может находиться на различных этапах проекта.

Фаза реализации проекта. Как только проект утвержден, начинается реальная работа. В терминах цикла управления проектом, мы завершили этапы планирования и переходим к этапам реализации. Реализация проекта начинается с формирования рабочей группы по проекту, после этого следует детальная разработка и распределение рабочих заданий, сметы. Реализация завершается, когда конечный продукт, полученный в результате выполнения проекта, удовлетворяет требованиям проекта. В процессе реализации проекта, вне зависимости от методологии, параллельно выполняется фаза или процессы по мониторингу и контролю состояния проекта. Еще один из важных процессов данного этапа – **управление изменениями**. Основные документы на данном этапе – отчеты по статусу проекта, выполненным работам, использованию ресурсов.

После реализации, проект подходит к **финальной стадии – завершению**. Проект является завершенным с точки зрения достижения поставленных целей проекта и получения ожидаемых конечных результатов. Кроме этого владельцы проекта или руководство организации могут принять решение по досрочному завершению проекта, или изменение целей проекта приводящие к его завершению.

Подходы и методы управления проектами

Выбор правильной методологии управления проектами (Project Management Methodologies PMM) – первый шаг к успеху вашей команды. Управление проектами помогает улучшать их реализацию с точки зрения эффективности и затрат, одновременно снижая риски. Но одного лишь декларирования приоритетов для этого недостаточно. Нужно хорошо понимать, какое позитивное воздействие оказывает каждая из методологий управления проектами и чем она может помешать успешной реализации проекта.

В этой главе мы коротко рассмотрим наиболее популярные методологии управления проектами и более подробно остановимся на наиболее интересных с моей точки зрения.

Процессно-ориентированное проектное управление (Process-Based Project

Management PBPM)

На сегодняшний день является основным подход к концепции управления проектом, основанный на процессном подходе к управлению проектами. Данный подход гарантирует того, что каждый проект будет направлен на продолжение следованию миссии компании. Перед стартом (инициацией) проекта, план проекта анализируется с целью определения его соответствия утвержденной или установленной миссии. Если же результат анализа отрицателен, то все стратегии и цели корректируются. Каждое действие добавляет ценность к стратегическому видению организации. Данные методы управления проектами также подходят и для административных проектов в компаниях.

Классическая Методология Управления Проектами «ВОДОПАД» (WATERFLOW)

«ВОДОПАД» (WATERFLOW) – Традиционная, классическая методология управления проектом. Она также носит название «каскадной» или «поточной» модели, вследствие того, что предлагаемая ею последовательность фаз напоминает водопад. Наиболее очевидный способ сделать свой проект более управляемым – это разбить его процессы реализации на последовательные этапы. Именно на такой линейной структуре базируется традиционное проектное управление. Данный подход не предполагает возврата к предыдущим этапам по их завершению и принятию, или внесение изменений в требования проекта. Данная методология управления проектами предполагает разбиение проекта на ряд последовательных задач, с четким определением целей и сроков. Члены проекта выполняют задания в установленном порядке, завершая каждое задание перед тем, как преступать к последующему. В «водопадной» модели, в применении к ИТ проектам разработки программного обеспечения, стадии идут в следующем порядке:

- Определение требований
- Проектирование
- Конструирование («реализация» или «кодирование»)
- Интеграция
- Тестирование и отладка («верификация»)
- Инсталляция
- Поддержка



При этом разработчик не может перейти к следующей стадии, не закончив предыдущую. Сначала полностью завершается этап «определение требований», в результате

чего получается список требований к программному обеспечению. После того как требования полностью определены, происходит переход к проектированию, в ходе которого создаются документы, подробно описывающие для программистов способ и план реализации указанных требований. После того как проектирование полностью выполнено, программистами выполняется реализация полученного проекта. На следующей стадии процесса происходит интеграция отдельных компонентов, разрабатываемых различными командами программистов. После того как реализация и интеграция завершены, производится тестирование и отладка продукта; на этой стадии устраняются все недочёты, появившиеся на предыдущих стадиях разработки. После этого программный продукт внедряется и обеспечивается его поддержка – внесение новой функциональности и устранение ошибок.

Сильные стороны классического проектного менеджмента – является то, что он требует от заказчика или руководства компании определить, что же они хотят получить, уже на первом этапе проекта. Раннее включение приносит определённую стабильность в работу проекта, а планирование позволяет упорядочить реализацию проекта. Кроме того, этот подход подразумевает мониторинг показателей и тестирование, что совершенно необходимо для реальных проектов. Потенциально, классический подход позволяет избежать стрессов ввиду наличия запасного времени на каждом этапе, заложенного на случай каких-либо осложнений и реализации рисков. Кроме того, с правильно проведённым этапом планирования, руководитель проектов всегда знает, какими ресурсами он обладает, даже если эта оценка не всегда точная. Основные преимущества: возможность заранее посчитать стоимость реализации решения и контроль состояния на всех этапах жизненного цикла управления проектом.

Слабые стороны классического проектного менеджмента – не толерантность к изменениям. Если в вашем проекте ресурсы и время не являются ключевыми ограничениями, а содержание проекта подвержено изменениям – возможно вам стоит присмотреться к другим системам управления проектами. Кроме этого, в реальных ИТ проектах довольно сложно на начальном этапе сформулировать детальные требования к конечному проекту.

Гибкая Методология Управления Проектами (Agile Project Management Methodology)

AGILE – семейство процессов и методов разработки гибких методов управления и ведения проектов. Сам по себе Agile – скорее набор идей и принципов того, как нужно реализовывать проекты. Уже на основе этих принципов и лучших практик были разработаны отдельные гибкие методы или, как их иногда называют – фреймворк (frameworks). Примеры: Scrum, Kanban, Crystal, LeSS, SAFe, Nexus и многие другие. Эти методы могут достаточно сильно отличаться друг от друга, но они следуют одним и тем же принципам. Гибкие методы предполагают изменения требований к продукту в течении всего времени проекта. Такое проектирование подразумевает совершенно иной подход к управлению проектами. Изначально методология разрабатывалась для проектов, которым требуются высокая гибкость и быстрая реализация. Гибкое управление проектом представляет собой поступательную и итеративную проектную методологию. Ее главной особенностью является то, что в начале выполнения проекта точно неизвестно, каким должен быть конечный продукт и каким будет жизненный цикл проекта. Вместо этого, проектная деятельность разбивается на несколько итеративных фаз – короткие циклы, называемые «спринтами». Каждый спринт состоит из множества задач и имеет свой конечный продукт и результат. Методология Agile позволяет менеджерам проектов постоянно получать обратную связь и улучшать продукт после каждой итерации. В соответствии с данной методологией управления проектами, ответственность за результат делится между тремя ролями:

- *Владелец продукта* – определяет проектные цели, разрабатывает оптимальный график

при заданных проектных параметрах, адаптирует процесс выполнения проекта к изменившимся требованиям и устанавливает приоритеты в характеристиках продукта

- *Scrum мастер* – устанавливает приоритеты в выполнении задач командой проекта и устраняет возникающие затруднения, препятствующие этому

- *Члены команды* – выполняют большинство поставленных задач, осуществляют ежедневный менеджмент, создают отчеты о ходе выполнения проекта, контролируют качество продукта.

Методология Agile является гибкой и позволяет легко изменить параметры проекта, что является значимым для таких сервисно-ориентированных проектов, как разработка программного обеспечения или графический дизайн. Но это методология не подходит для проектов со строго заданными параметрами и требованиями.



В процессе управления проектом важно умение быстро адаптироваться к изменениям, отслеживать последние тенденции развития и уметь извлекать из них выгоду. Не менее важным является и человеческий ресурс. Поэтому и необходимо умение создавать динамичную команду проекта на основе сотрудничества и гибкости, возможности нахождения компромисса. Немаловажную роль играют заинтересованные стороны (Stakeholders). Они контролируют и проверяют проект на каждой стадии, а члены команды, с свою очередь, правильно и своевременно корректируют проект, создавая высококачественные продукты или услуги, соответствующие потребностям и запросам потребителей.

AGILE-проектирование лучше подходит для проектов, требующих интенсивного взаимодействия в реальном времени и реализуемых высокомотивированными командами, не нуждающимися в дополнительном контроле. Методология AGILE отличается высокой интерактивностью, дает возможность быстро подстраиваться под проект. Одно из главных ее преимуществ в том, что можно быстро выявлять спорные моменты и вносить необходимые изменения на ранней стадии разработки, не дожидаясь завершения тестирования. AGILE – проектирование обеспечивает применение повторяющихся процессов, снижение рисков, оперативную обратную связь, быструю оборачиваемость и уменьшение сложности.

Сильные стороны Agile – их гибкость и адаптивность. Он может подстроиться под практически любые условия и процессы организации. Именно это обуславливает его нынешнюю популярность и то, сколько систем для различных областей было создано на его

основе. Один из принципов Agile: «Реакция на изменения важнее следования плану». Вотчина Agile – разработка новых, инновационных продуктов с «открытым концом». В проектах по разработке таких продуктов высока доля неопределённости, а информация о продукте раскрывается по ходу проекта. В таких условиях реализовывать проект по «водопадку» становится невозможно – нет информации для планирования. Второй сильной стороной подхода является возможность «совершать ошибки» и быстро их исправлять без существенного влияния на статус проекта в целом.

Слабая сторона состоит в том, что каждой команде придётся самостоятельно составлять свою систему управления, руководствуясь принципами Agile. Это непростой и длительный процесс, который потребует изменений всей организации, начиная процедурами и заканчивая базовыми ценностями. Это тернистый путь и не всем организациям он под силу. Этот путь потребует от лидера изменений не только знаний и упорства, но и серьёзных административных ресурсов, а также затрат. Кроме этого – плавающая оценка сроков и бюджетов, неопределенность планирования целей и задач, недостаточное документирование и как следствие увеличение вероятности расхождения поставленных задач и фактической реализации, сложность ретроспективного анализа проекта.

Метод SCRUM семейства Гибких Методов Управления Проектами

SCRUM – («схватка») классический метод, с описанием процессов планирования, контроля и анализа на всех этапах ведения проекта, базирующийся на идеях Agile. Методология реализации agile-разработки предполагает использование интерактивного подхода. «Скрам-сессии», или «30-дневные спринты», используются для определения приоритетных задач. Роль менеджера проекта для упрощения передается скрам-мастеру. Для независимого решения конкретных задач формируются небольшие команды. В ходе встреч со скрам-мастером оцениваются достигнутые результаты, после чего определяется приоритетность невыполненных задач. Основная особенность методики:

- Совещания и анализ по определённым отрезкам времени «спринтов» (sprints).
- Небольшая команда
- Ограничение по определённым промежуткам времени (sprint) для выполнения WIPs.
- Определённых «кусоч» продукта (Work in Process WIPs)

Следуя заветам Agile, Scrum разбивает проект на части, которые сразу могут быть использованы Заказчиком для получения ценности, называемые заделами продуктов («W» – product backlog). Затем владельцем продукта – представителем заказчика в команде определяются приоритеты этих частей. Самые важные «кусочки» первыми отбираются для выполнения в спринте – так называются итерации в Scrum, длящиеся от 2 до 4 недель. В конце спринта заказчику представляется рабочий инкремент продукта – те самые важные «кусочки», которые уже можно использовать. Например, сайт с частью функционала или программа, которая уже работает, пусть и частично. После этого команда проекта приступает к следующему спринту. Длительность у спринта фиксированная, но команда выбирает её самостоятельно в начале проекта, исходя из проекта и собственной производительности.

Чтобы удостовериться в том, что проект отвечает требованиям заказчика, которые имеют свойство изменяться со временем, перед началом каждого спринта происходит переоценка ещё не выполненного содержания проекта и внесение в него изменений. В этом процессе участвуют все – команда проекта, лидер команды проекта (Scrum Master) и владелец продукта. И ответственность за этот процесс лежит на всех. Scrum Мастер призван помочь участникам проекта лучше понять и принять ценности, принципы и нормы практики Scrum. Он лидер и посредник между внешним миром и командой. Его задача – следить, чтобы никто не мешал команде самостоятельно и комфортно работать над

поставленными задачами. Команда же отвечает за то, чтобы в конце спринта все необходимые задачи были сделаны, а поставки – выполнены. Основная структура процессов Scrum вращается вокруг 5 основных встреч:

- упорядочивания заделов (backlog),
- планирования Спринта,
- ежедневных летучек
- подведения итогов Спринта
- ретроспективы Спринта.

Встреча по упорядочиванию заделов (Backlog Refinement Meeting, «Backlog Grooming»): Эта встреча аналогична фазе планирования в классическом проектном управлении, и проводится в первый день каждого Спринта. На ней рассматривается – что уже было сделано по проекту в целом, что ещё осталось сделать и принимается решение о том, что же делать дальше. Владелец продукта определяет, какие задачи на данном этапе являются наиболее приоритетными. Данный процесс определяет эффективность Спринта, ведь именно от него зависит, какую ценность получит Заказчик по итогам спринта.

Планирование Спринта: После того, как Владелец продукта определил приоритеты, команда совместно решает, что же конкретно они будут делать во время грядущей итерации, как достигнуть поставленной на предыдущей встрече цели. Команды могут применять различные инструменты планирования и оценки на данном этапе, лишь бы они не противоречили принципам и логике Scrum. Планирование Спринта проводится в самом начале итерации, после Встречи по упорядочиванию продукта.

Ежедневные летучки: Каждый день спринта, в идеале, в одно и то же время, члены команды тратят 15 минут на то, чтобы поделиться информацией о статусе задач и состоянии проекта. На ней не происходит обсуждений проблем или принятия решений – если после встречи возникают вопросы и конфликты, Scrum Мастер и вовлечённые участники обсуждают их отдельно. Летучка же нужна для обмена информацией и поддержания всех членов команды в курсе состояния проекта.

Подведение итогов Спринта: Цель этапа – обследование и адаптация создаваемого продукта. Команда представляет результаты деятельности всем заинтересованным лицам. Основная задача – убедиться, что продукт этапа соответствует ожиданиям участников и согласуется с целями проекта.

Ретроспектива Спринта: Проводится сразу после Подведения итогов спринта и до планирования следующего спринта. На нём команда выясняет, насколько чётко и слаженно проходил процесс реализации этапа. Обследованию подвергаются возникшие проблемы в работе, методологии и взаимодействии. Именно этот этап позволяет команде провести рефлексию и следующий Спринт провести эффективнее.

Сильные стороны – был разработан для проектов, в которых необходимы «быстрые победы» в сочетании с толерантностью к изменениям. Кроме того, этот фреймворк подходит для ситуаций, когда не все члены команды имеют достаточный опыт в той сфере, в которой реализуется проект – постоянные коммуникации между членами командами позволяют недостаток опыта или квалификации одних сотрудников за счёт информации и помощи от коллег. На мой взгляд основное преимущество Scrum в том, что он позволяет «быстро ошибаться». Вместо того, чтобы долго и с большими затратами готовить крупный релиз, поставки раз в две недели по Scrum имеют небольшой размер. Их легко отслеживать и, если что-то идёт не так, быстро исправлять.

Слабые стороны – очень требователен к команде проекта. Она должна быть небольшой (5—9 человек) и кросс-функциональной – то есть члены команды должны обладать более чем одной компетенцией, необходимой для реализации проекта. Например, разработчик ПО должен обладать познаниями в тестировании и бизнес-аналитике. Делается это для того, чтобы часть команды не «простаивала» на разных этапах проекта, а также для того, чтобы сотрудники могли помогать и подменять друг друга. Кроме того, члены команды

должны быть «командными игроками», активно брать на себя ответственность и уметь само-организовываться.

Подобрать такую зрелую команду очень непросто! Scrum подходит не для всех команд и организаций ещё и потому, что предлагаемый процесс может не подойти для разработки конкретного продукта – например промышленного станка или постройки здания.

Метод KANBAN семейства Гибких Методов Управления Проектами

KANBAN – также представляет из себя гибкий, итеративно-инкрементальный подход к управлению проектами базирующийся на идеях Agile. Является противоположностью «SCRUM» метода. Основные особенности методики:

- Каждый участник проекта самостоятельно берет на себя ограниченное количество задач, а не по указанию менеджера
- Работа вносится в карточку (Sticker)
- Количество «незавершённой» работы (WIPs) ограничено для каждой стадии
- Новая работа берется только тогда, когда существующая выполнена или «вытянута» (LEAN).
- Больше внимания к управлению изменениями, визуализация узким мест, незавершенной работы и т.п.
- Ограничения по количеству WIPs и их статусы

Lean выглядит немного абстрактным сам по себе, но в комбинации с Kanban его становится гораздо проще использовать для построения собственной системы управления проектами. Kanban очень похож на схему промышленного производства. На входе в этот процесс попадает кусочек металла, а на выходе получается готовая деталь. Также и в Kanban, инкремент продукта передаётся вперёд с этапа на этап, а в конце получается готовый к поставке элемент. Руководство принципом – «держи на полках только то, что нужно клиенту». А потому в Kanban разрешается оставить неоконченную задачу на одном из этапов, если её приоритет изменился и есть другие срочные задачи – всё это нормально для работы по Kanban.

Kanban намного менее строгий, нежели Scrum – он не ограничивает время спринтов, нет ролей, за исключением владельца продукта. Kanban даже позволяет члену команды вести несколько задач одновременно, чего не позволяет Scrum. Также никак не регламентированы встречи по статусу проекта – можно делать это как Вам удобно, а можно не делать вообще.

Для работы с Kanban необходимо определить этапы потока операций (workflow). В Kanban они изображаются как столбцы, а задачи обозначают специальные карточки. Карточка перемещается по этапам, подобно детали на заводе, переходящей от станка к станку, и на каждом этапе процент завершения становится выше. На выходе мы получаем готовый к поставке заказчику элемент продукта. Доска со столбцами и карточками может быть, как настоящей, так и электронной – даже здесь Kanban не накладывает никаких ограничений на пользователей. Ваша собственная система Kanban может быть настолько гибкой, насколько Вы сами того пожелаете – ведь во многом Kanban является визуализацией идеи Agile.

Но у Kanban есть четыре столпа, на которых держится вся система:

- *Карточки:* Для каждой задачи создается индивидуальная карточка, в которую заносится вся необходимая информация о задаче. Таким образом, вся нужная информация о задаче всегда под рукой.
- *Ограничение на количество задач на этапе :* Количество карточек на одном этапе строго регламентировано. Благодаря этому сразу становится видно, когда в потоке операций возникает «затор», который оперативно устраняется.
- *Непрерывный поток:* Задачи из беклога попадают в поток в порядке приоритета. Таким образом, работа никогда не прекращается.

•*Постоянное улучшение* («кайзен» (kaizen)): Концепция постоянного улучшения появилась в Японии в конце XX века. Её суть в постоянном анализе производственного процесса и поиске путей повышения производительности.

Сильные стороны – Как и Scrum, Kanban хорошо подходит для достаточно сплочённых команды с хорошей коммуникацией. Но в отличие от Scrum, в Kanban нет установленных чётких временных рамок, что хорошо подходит для замотивированных и опытных команд. При правильной настройке и управлении, Kanban может принести большую пользу команде проекта. Точный расчёт нагрузки на команду, правильная расстановка ограничений и концентрация на постоянном улучшении – всё это позволяет Kanban серьёзно экономить ресурсы и укладывать в сроки и рамки бюджета. И всё это в сочетании с гибкостью.

Слабые стороны – Часто можно слышать, что по Kanban, в отличие от Scrum, можно работать с практически любой командой. Но это не совсем так. Kanban лучше всего подходит для команд, навыки членов которых пересекаются друг с другом. Таким образом они могут помогать друг другу преодолевать трудности при решении задач. Без этого Kanban будет не так эффективен, как мог бы быть. Также, как уже было сказано, Kanban лучше подходит в тех случаях, когда нет жёстких сроков. Для жёстких сроков проекта лучше подходит классический подход или Scrum.

Гибридная Методология Управления Проектами

Несмотря на то что многие команды отдают предпочтение либо методологии водопада, либо agile-проектированию, преимущества обоих подходов привели к появлению гибридной методологии, когда этапы планирования и определения требований выполняются согласно методологии водопада, а этапы проектирования, разработки, внедрения и оценки соответствуют гибкому подходу. Данная методология является попыткой применения сильных сторон каждого из основных подходов, а также снижения негативного воздействия слабых сторон. Гибридная методология может хорошо вписаться в сферу информационных технологий за счет того, что на уровне руководства организации проект имеет четко поставленные цели, хорошо документированы, предоставляет возможность мониторинга статуса проекта для предоставления руководству. На этапе выполнения за счет высокого уровня коммуникации между представителями бизнеса и непосредственно исполнителями задачи по проекту глубоко детализированы, понятны разработчикам. Возможность учиться «на лету», совершать ошибки и совершенствовать продукт под текущие требования бизнеса одинаково хорошо для разработчиков и бизнеса. Конечно за все надо платить. Подход предъявляет требования к как к техническому уровню подготовки сотрудников, так и к его персональным качествам.



Из собственной практики управления проектами в ИТ департаменте, данный подход не стоит внедрять в самом начале, но по мере совместной работы сотрудников ИТ департамента и бизнеса по нескольким проектам, так сказать «притирки» сотрудников данный метод будет являться логическим продолжением и будет наиболее эффективным, и результативным.

Прочие методы и специфические подходы к Управлению Проектами

Методология Быстрой Разработки Приложений (Rapid Application Development RAD)

Быстрая разработка приложений (RAD) – это специфическая проектная методология, чаще всего используемая в проектах по разработке ПО, основной целью которых является быстрое и качественное создание приложения.



Диаграмма: Сравнение WATERFLOW и RAD подходов

Суть методологии – подход к созданию средств разработки программных продуктов, уделяющая особое внимание скорости и удобству программирования, созданию технологического процесса, позволяющего программисту максимально быстро создавать компьютерные программы. Практическое определение: RAD – это жизненный цикл процесса проектирования, созданный для достижения более высокой скорости разработки и качества ПО, чем это возможно при традиционном подходе к проектированию. Данная методология управления проектами выделяет четыре стадии проекта:

- Планирование
- Пользовательское проектирование
- Быстрое конструирование
- Переключение

Основные преимущества применения различных подходов RAD:

•*Применение итеративного подхода* к разработке решений. Итеративный подход предполагает выполнение работ параллельно с непрерывным анализом полученных результатов и корректировкой предыдущих этапов работы, то есть своего рода обратную связь. Проект при этом подходе периодически проходит повторяющийся цикл Планирование-Реализация-Проверка-Оценка. Благодаря применению итеративного подхода, RAD может быстро реагировать на изменяющиеся требования бизнеса.

•*Инкрементальный подход* предполагает разработку услуги «от куска к куску», то есть последовательно. При этом каждый «кусочек» может поддерживать одну из бизнес-функций, для которых предназначена услуга в целом. Для бизнеса инкрементальный подход дает возможность использования какой-то значимой части услуги до того, как она будет разработана полностью. Дополнительные преимущества: продукт быстрее поступает на рынок, более широкие возможности для разработки устраивающего пользователей интерфейса, большая адаптивность к изменяющимся требованиям бизнеса и простота развития и изменения функциональности решения. Методология быстрой разработки приложений, с одной стороны, помогает улучшить показатели результативности проекта и повысить качество риск-менеджмента. Но с другой стороны, данная методология не подходит для масштабных IT проектов, может привести к низкому качеству кода и требует постоянного вовлечения клиента в процесс исполнения всего проекта. RAD является более современным и гибким подходом к проектированию.

Недостатки метода – слабая документная база может приводить к недопониманию, ошибкам при формировании и разработки, сложность контроля и аудита процесса разработки. При проектировании услуг возможно комбинирование инкрементального и итеративного подходов. Начинают с определения требований для услуги в целом, продолжают путем инкрементальной разработки отдельных ее частей.

Методология Экстремального Программирования (Extreme Programming XP)

Данная методология управления проектами оказывает особенности (возможности) коротких циклов развития, частые релизы и открытое взаимодействие со стейкхолдерами. Команды сосредотачиваются на сотрудничестве, эффективности и производительности, написании наиболее простых из всех возможных кодов для достижения желаемого качества, при этом избегая истощения и низкого качества конечного результата.

Методология моделирования событий Event Chain Methodology (ECM)

Эта методология управления проектами помогает выявить и спрогнозировать потенциальные риски. Анализ проекта при помощи метода Монте Карло и Диаграммы цепочки событий помогает определить вероятность некоторых рисков и их возможное влияние на проект в целом. Визуализация связей между внешними событиями и работами проекта помогает создать план, максимально приближенный к реальности.

Метод Адаптивные Рамки Проектов APF (Adaptive Project Framework)

Использование адаптивных/регулируемых рамок проектов APF (Adaptive Project Framework) позволяет улучшать проект на каждом этапе, основываясь на полученном опыте от предыдущих результатов. Определив цели проекта и постоянно контролируя работы проекта, менеджер может обеспечить успех максимально возможной стоимости бизнеса и создать бизнес-ценность для потенциального потребителя.

Метод «Реализация Выгоды» (Benefit Realization BF)

Цель метода «Реализация Выгоды» (Benefit Realization BF) – выгода от реализации проекта. Успех определяется как достижение желаемой/ожидаемой выгоды. Если клиенты хотят увеличить продажи CRM (система управления взаимоотношениями с клиентами – customer relationship management software), проект не будет выполнен/реализован до того момента, пока продажи не повысятся на 15% – даже если Вы установили и наладили работу CRM вовремя и с соблюдением/в соответствии с бюджетом.

Методология PRISM (проекты со встроенными устойчивыми/жизнеспособными методами)

Сочетание проектного планирования с экологической устойчивостью мер. Хотите пойти в «зеленом» направлении? В таком случае, PRISM точно для Вас! Сокращение расходования энергии и издержек обращения (распределение затрат), все это при одновременном снижении Вашего воздействия на окружающую среду.

Помимо перечисленных, существуют и другие методологии управления проектами:

- функционально-ориентированная разработка (feature driven development, FDD),
- разработка динамических систем (dynamic systems development, DSDM),
- адаптивная разработка программного обеспечения, Rational Unified Process (RUP),
- Концепции Шесть сигм (six sigma) и Бережливого Производства (LEAN). Управление проектом на основе принципов «контроля качества». Будут детально рассмотрены в следующей главе.

Методология Управления Проектами в Контролируемой Среде (PRINCE2)

PRINCE2 (Projects in Controlled Environments PRINCE2) так же является структурированной методологией к проектному управлению. Это одна из самых популярных методологий управления проектами, широко используемая в Великобритании в управлении как в бизнесе, так в органах власти. PRINCE2 – это процессно-ориентированная проектная методология (PBPM), которая фокусируется на процессах верхнего уровня (управление, организация, контроль), а не на низших задачах (декомпозиция работ, разработка графиков).

Методология PRINCE2 базируется на семи принципах, семи темах и семи процессах. Принципы являются центральным элементом методологии: если хотя бы один из них не выполняется, то нельзя говорить, что проект выполняется в рамках PRINCE2.

Принципы методологии PRINCE2

Постоянная оценка экономической необходимости – остается ли неизменной экономическая выгода от проекта на протяжении всего жизненного цикла проекта.

Обучение на опыте – команда проекта должна постоянно искать и изучать опыт предыдущих проектов

Определение ролевой модели – команда проекта должна иметь ясную организационную структуру и вовлекать подходящих людей для решения нужных задач

Управление по этапам – необходимо, чтобы проекты были спланированы, а также подвергались мониторингу и контролю на каждом этапе выполнения;

Управление по отклонениям – следует четко обозначить допустимые границы отклонений в проекте, чтобы установить границы ответственности.

Фокус на продуктах – необходимо концентрироваться на определении и достижении результатов проекта.

Адаптация к проектной среде – следует адаптировать процессы и инструменты управления проектом к требованиям проектной среды, а также к масштабу работ, их сложности, важности, квалификационным требованиям и степени риска.

PRINCE2 – гарантирует, что каждый проект имеет бизнес обоснование и способствует

созданию ценности. Планирование начинается с четкого определения: потребностей, запрашиваемых потребителем, реальной выгоды и точной оценки затрат.

Темы методологии управления проектами PRINCE2

Обоснование проекта: какую ценность проект принесёт организации?

Организация: каким образом необходимо распределить роли и ответственность между членами проектной команды для того, чтобы эффективно управлять проектом.

Качество: какие имеются требования и критерии к качеству и каким образом можно их обеспечить

Планы: шаги, требуемые для разработки плана, и инструменты PRINCE2, необходимые к использованию

Риски: каким образом менеджмент проекта будет разрешать проблему наличия неопределённостей в плане проекта и во внешней среде.

Изменение: как руководство проекта будет оценивать влияние непредвиденных задач и изменений и реагировать на них

Прогресс: реализуемость проекта, выполнение планов и дальнейшее развитие проекта

Семь процессов управления PRINCE2

И наконец, PRINCE2 подразумевает следующие семь процессов управления проектом:

- запуск проекта
- руководство проектом
- инициация проекта
- контроль этапов
- управление созданием продукта
- управление границами этапов
- закрытие проекта

PRINCE2 позволяет стандартизировать процедуры управления проектами, улучшить координацию деятельности, а также помогает понять, каким образом следует планировать проект и осуществлять мониторинг его выполнения, что следует делать, если план проекта не выполняется. Однако методология PRINCE2 не является лучшим выбором для проектов небольшого масштаба или для проектов с большей степенью вероятности изменений объема работ и требований к ним.

Сильные стороны PRINCE2 :

- Адаптируемость к особенностям организации;
- Наличие чёткого описания ролей и распределения ответственности;
- Акцент на продуктах проекта;
- Определённые уровни управления;
- Фокус на экономической целесообразности;
- Последовательность проектной работы;
- Акцент на фиксации опыта и постоянном совершенствовании.

Слабые стороны PRINCE2 – Отсутствие или нехватка отраслевых практик и отсутствие конкретных инструментов для работы.

Управление проектами на основе методологии «PROJECT MANAGEMENT INSTITUTE PMI»

Общие положения

Данная методология является представителем Процессно-ориентированное подходом

у Управлению Проектами (Process-Based Project Management PBPM) и основывается на методологии традиционного, классического подхода к управлению проектами. Наиболее очевидный способ сделать свой проект более управляемым – это разбить процесс его исполнения на последовательные этапы. Именно на такой линейной структуре базируется традиционное проектное управление. Все процессы в руководстве PMBooK разделяются на следующие группы (фазы):

Группа процессов инициации проекта (Initiating)

На данном этапе часто проводятся совещания и «мозговые штурмы», на которых определяется что же должен представлять из себя продукт проекта. В некотором смысле самой важной частью проекта является его начало. Именно на этой стадии «бросается жребий»: либо проект хорошо разработан и может быть выполнен в сроки, установленные высшим руководством, и в рамках выделенных средств, либо он не имеет перспектив и обречен на провал с самого начала. Эта часть проекта – не место для опрометчивых обещаний в попытке предстать героем. Скорее это время для рационального и творческого подхода к формулировке начальных требований к проекту с целью избежать тупиковых ситуаций. Следует помнить, что после того как вы поставили цель проекта, руководство будет ожидать от вас ее достижение.

Группа процессов инициации состоит из процессов, способствующих формальной авторизации начала нового проекта.

- Разработка Устава проекта (Develop Project Charter)
- Определение заинтересованных сторон (Identify Stakeholders)

Группа процессов планирования проекта (Planning)

Определяет и уточняет цели и планирует действия, необходимые для достижения целей и содержания, ради которых был предпринят проект. Планирование – это определение ясных и точных задач, и как следствие рабочих заданий, служащих для достижения конечной поставленной цели. Цель может представлять собой решение какой-нибудь проблемы или достижение некоторого состояния или условия, отличного от существующего. На данном этапе команда решает, как она будет достигать цели, поставленной на предыдущем этапе. На данном этапе команда уточняет и детализует цели и результаты проекта, а также состав работ по нему. На основании данной информации формируется календарный план и бюджет, оценивает риски и уточняются заинтересованные стороны. Планирование проекта может потребовать значительных затрат времени, сил и ресурсов, в зависимости от его размера. Опыт показывает, что усилия и ресурсы могут быть потрачены впустую, если не осуществить надлежащего планирования конкретного проекта перед принятием решения о том, реализовывать ли его или нет.

Организация проекта является первостепенной задачей по управлению проектом. Необходимо определение владельца проекта – человек или группа, обладает авторитетом по принятию решений, назначить менеджера проекта и сформировать рабочей группы, определить порядок управления и взаимодействия по проекту, а также выделить соответствующих полномочий руководителю проекта и рабочей группе. Управление проектом за пределами функциональных границ организации одна из задач руководителя проекта. Ему приходится общаться, подавать идеи, вести переговоры, решать проблемы и разрешать конфликты за пределами функциональных, а иногда и географических границ организации. Постановка задачи, обоснование необходимости в проекте и описание его возможностей позволяют сформулировать цель проекта. Такая формулировка может быть очень краткой, но точной. Постановка задач по проекту важна по двум причинам:

- Задача четко определяет, что должно быть сделано для достижения целей
- Задача является событием, срок окончания которого можно определить.

Метод «SMART» помогает сформулировать цели и задачи проекта как:

- *Specific* – Быть точным при постановке цели
- *Measurable* – Установить измеримые показатели состояния
- *Assignable* – Иметь возможность поручить выполнение задания кому-нибудь
- *Realistic* – Определить, могут ли быть реально выполнены в срок и в рамках выделенных ресурсов
- *Time related* – Определить временные рамки, т. е. продолжительность ее выполнения

Для достижения поставленной цели, необходимо выполнить несколько основных задач проекта. Эти задачи являются частными целями и представляют собой основные компоненты проекта (иногда используется термин «вехи» или milestone). Частные цели не являются фактическими рабочими заданиями, выполняемыми в рамках проекта, а представляют собой контрольные точки, задающие направление работ. Они точнее формулируются, чем основная цель, и также ориентированы на действия. Для достижения основной цели необходимо реализовать все частные цели.

Выделение ресурсов под проект. Не следует думать, что только деньги являются ресурсами. В качестве основных ресурсов можно выделить следующие:

- финансовые ресурсы (как прямые необходимые для реализации проекта, так и на управление проектом)
- людские ресурсы (кто, когда, как и на какой срок участвует в проекте)
- материальные ресурсы (имеющиеся в наличии, требуемые и т.п.)
- административные ресурсы (полномочия, организация)

Кроме этого в список необходимых ресурсов может быть включены изменения в организационной структуре компании, помещение под офис (для крупных проектов) и т.п. Из практики участия в проектах, можно выделить два наиболее вероятных сценария выделения ресурсов:

- Руководитель проекта определяет необходимые ресурсы на основе предварительного плана, в котором дается первичная оценка количества ресурсов, необходимых для проекта. Руководитель проекта сможет сформулировать требования к ресурсам и обсудить их с уполномоченным руководителем. Данный сценарий наиболее предпочтительный.

- Необходимые ресурсы назначаются без участия руководителя проекта. Часто из практики, у руководителя проекта может и не быть выбора, независимо от того, достаточно ли выделено ресурсов на проект или нет. Не следует идти на поводу у руководства, давая согласие на уровень поддержки, который явно недостаточен для реализации проекта. Осторожность и здравый смысл должны быть определяющими на этой ранней стадии.

Документ, содержащий обзор проекта, составлен, проанализирован с участием экспертов, а затем подан на рассмотрение высшего руководства организации. Следующий важный аспект управления проектом является процесс разбиения проекта на составные части, результатом которого является схема разбиения на рабочие задания (СРРЗ). СРРЗ – это иерархическое представление проекта. С помощью этой схемы руководитель проекта определяет задания, которые требуется выполнить, чтобы начать и закончить проект. На этом этапе у руководителя есть цель и ряд задач, которые необходимо выразить через задания и работы, подлежащие выполнению. Четко определенное задание имеет следующие характеристики:

- Его состояние и срок завершения легко определить, оно имеет четко определенное начало и конец
- Понятно, поскольку возможно выполнялось ранее, а время, требуемое для его выполнения, и связанные с ним затраты легко оценить, используя опыт, приобретенный при реализации похожих заданий в прошлом.

- Включает в себя работы, которые поддаются контролю и не зависят от работ, составляющих другие задания
- Как правило, составляет одну непрерывную последовательность работ.

Оценка времени выполнения каждого из заданий, составляющих проект. Время, требуемое для выполнения задания, является случайной величиной. Это значит, что если данное задание выполняется много раз, то можно ожидать, что время его выполнения будет несколько меняться. Это будет справедливо даже для регулярных заданий. Такой разброс объясняется следующими факторами:

- уровнем квалификации сотрудников, выполняющих задание
- использованием различного оборудования
- доступностью материалов
- непредвиденными событиями (болезнями, стихийными бедствиями, авариями, текучестью кадров и т. п.)

Известно, что подобные события могут происходить, но нельзя точно предсказать их появление при реализации конкретного проекта или задания. Тем не менее, их нужно как-то учитывать. Для этого можно использовать метод оценки критического пути.

Оценка затрат на задание. Существуют четыре основных категории затрат (хотя можно также использовать план бухгалтерских счетов организации), которые можно определить для каждого задания:

- Рабочая сила
- Материалы
- Другие прямые затраты (командировки, телефон, услуги по контрактам)
- Косвенные затраты (накладные расходы)

Далее необходимо определить последовательность выполнения заданий по проекту. Для простых проектов можно выполнять задания по одному по порядку. Другой путь – провести анализ всех заданий и определить, какие из них необходимо завершить до начала выполнения других. Такой анализ позволяет выявить порядок, в котором можно одновременно выполнять несколько заданий. Методом критического пути (МКП) определяет последовательность одновременно выполняемых заданий, который позволяет завершить проект в установленные сроки. Выявление критических заданий, определение критического пути и построение диаграмма приоритетов – представить проект в графическом виде. Для этого необходимо освоить несколько простых правил построения схем проектов. Задание является основной «единицей анализа» в упорядоченной схеме. Задания представляются на схеме в виде прямоугольников, называемых «узлами заданий». Символы, изображенные в прямоугольнике, описывают временные свойства задания. Некоторые из них описывают характеристики самого задания (например, номер задания), тогда как другие представляют собой расчетные величины (ES, EF, LS, LF), связанные с заданием. Время выполнения проекта – это самый длинный временной путь на схеме. Последовательность заданий, составляющая самый длинный путь, называется критическим путем. До тех пор, пока задания, находящиеся на критическом пути, выполняются в срок, проект идет по графику. Определим теперь четыре расчетных параметра (ES, LS, EF, LF), связанные с каждым узлом задания. Следующие расчетные величины будут использованы для определения времени выполнения проекта и критического пути:

Самое раннее время начала (ES) выполнения задания – это самый ранний момент времени, когда все предшествующие ему задания уже завершены и можно приступить к выполнению данного задания. Время ES для задания, у которого нет предшествующих заданий, условно принимается равным нулю.

Самое раннее время окончания (EF) задания равно времени ES плюс предполагаемое время выполнения задания. Время ES для задания, которому предшествует одно задание,

представляет собой время EF для этого предшествующего задания. Время ES для заданий, которым предшествуют два и больше заданий, является максимальным из времен EF для этих предшествующих заданий.

Самое позднее время начала (LS) и самое позднее время окончания (LF) задания – это самые поздние моменты времени, когда можно начать (LS) или закончить (LF) задание, не увеличивая время выполнения проекта в целом.

Чтобы рассчитать эти моменты, будем двигаться по схеме назад. Сначала примем время LF для последнего задания на схеме в качестве времени EF рассматриваемого задания. Время LS для данного задания равно его времени LF минус предполагаемое время выполнения этого задания. Время LF для всех непосредственно предшествующих заданий является минимальным из времен LS для всех заданий, для которых рассматриваемое задание является предшествующим. Необходимо рассчитать еще одну величину, называемую резервом времени для задания.

Резерв времени – это допустимая величина задержки начала или окончания задания, которая не приводит к задержке выполнения проекта в целом. Резерв времени математически представляет собой разность $LS - ES$ (или $LF - EF$, что-то же самое). По определению, последовательность заданий, имеющая нулевой резерв, является критический путь.

Техническое задание по проекту – представляет собой переход от этапа планирования (определение, составление плана) к этапам реализации (организация, контроль, завершение). Как будет показано далее, техническое задание представляет собой фундамент, на котором основана внутренняя согласованность проекта и который обеспечивает базис для принятия всех административных решений. Рассмотрим техническое задание, уделив особое внимание составляющим его частям и их использованию в качестве средств управления. Техническое задание проекта предназначено для того, чтобы получить:

- изложение возникшей проблемы, принимаемого общего подхода к ее решению и ожидаемых в результате выгод;
- полное описание заданий по проекту, необходимых затрат времени и ресурсов;
- такое подробное описание необходимо администрации, чтобы решить, следует ли перейти к этапам реализации проекта
- динамичный инструмент для руководителя проекта и рабочей группы, который будет использоваться для принятия решений в течение всего времени работы над проектом;
- справочную документацию для административного контроля;
- средство, с помощью которого можно ознакомить с проектом и подготовить к его выполнению новых членов рабочей группы по проекту;
- документ-сводку для тех представителей вашей организации, кто, не работая над проектом непосредственно, должны все-таки иметь о нем представление.

Очевидно, что задание – это ключевой документ в проекте. Техническое задание должно быть написано так, чтобы его понимали и использовали и вышестоящая администрация, и руководители проекта, и члены рабочей группы, и другие руководители, а также специалисты, которым необходима эта информация. **Составляющие технического задания проекта :**

- Название проекта
- Цели проекта
- Руководитель проекта
- Владелец проекта или заинтересованные лица
- Состав рабочей группы
- Задания – Этот раздел состоит из трех подразделов: номер задания, краткое, но смысловое имя, присвоенное заданию и описание задания. В нем должно содержаться в (точных выражениях) конкретное изложение содержания работы, которую необходимо выполнить.
- Оценочные даты начала и завершения работ.

- График выполнения проекта
- Смета проекта – Информация о смете в этом отчете обобщается на уровне задания.
- Метрики и критерии достижения целей
- Дополнительные условия

Все проекты имеющие финансовые аспекты получения прибыли, могут потребовать тщательной оценки влияния проекта на доходы и расходы, перед тем как утверждать проект,

План сроков и хода работ – это график, в котором для каждого рабочего пакета указывается срок начала и окончания, а также запланированная продолжительность. Как правило план сроков и хода работ изображается в виде диаграммы Гантта и сетевых графиков, в которых задается логическая последовательность выполнения рабочих пакетов.

В группу процессов планирования входят следующие процессы:

- Разработка плана управления проектом
- План управления содержанием
- Сбор требований
- Определение содержания
- Создание иерархической структуры работ
- Разработка плана управления расписанием
- Определение операций
- Определение последовательности операций
- Оценка ресурсов операций
- Оценка длительности операций
- Разработка расписания
- Разработка плана управления стоимостью
- Оценка стоимости
- Определение бюджета
- Планирование качества
- Разработка плана управления человеческими ресурсами
- Планирование коммуникаций
- Планирование управления рисками
- Идентификация рисков
- Качественный анализ рисков
- Количественный анализ рисков
- Планирование реагирования на риски
- Планирование закупок
- Разработка плана управления заинтересованными сторонами

Группа процессов реализации проекта (Executing)

На этой фазе происходит собственно основная работа по проекту – написание кода, возведение здания и тому подобное. Следуя разработанным планам начинает создаваться содержание проекта, определённое ранее, проводится контроль по выбранным метрикам. Во второй части данной фазы происходит тестирование продукта, он проверяется на соответствие требованиям заказчика и заинтересованных сторон. В части тестирования выявляются и исправляются недостатки продукта.

Данная фаза включает в себя распределение обязанностей по выполнению рабочих заданий. Создание эффективно работающей группы – это в одинаковой степени и искусство, и наука. Чтобы создать эффективно работающую группу, необходимо принимать во внимание не только техническую квалификацию руководителя проекта и членов рабочей группы, но также их критические роли и взаимоотношения между ними. Выбор руководителя проекта и членов группы не будет совершенным – в любом решении

по кадровым вопросам всегда присутствует риск. Главная цель при выборе руководителя проекта – назначить на эту должность человека опытного, компетентного и способного получить конечный результат при соблюдении требований проекта в установленные сроки с имеющимися ресурсами. С этой точки зрения все основные качества эффективно работающего руководителя проекта можно отнести к одной из следующих пяти категорий:

- Образование и опыт
- Лидерство и стратегическое мышление
- Техническая компетентность
- Умение работать с людьми
- Доказанные способности к управлению

Выбор рабочей группы зависит от ряда факторов:

- от задачи и целей проекта
- от характера работы, которая должна быть сделана
- от квалификации, необходимой для найма, назначения, получения полномочий, контроля, связи и выполнения требуемой работы на каждом из этапов проекта
- наличия соответствующих кадров в организации, где будет выполняться проект

Руководителю проекта и членам рабочей группы важно знать, что вновь образованные группы проходят через цикл становление и эволюция рабочей группы, имеющие следующие названия:

•*Этап формирования* – члены рабочей группы знакомятся друг с другом, «ломается лед» и налаживаются отношения.

•*Этап привыкания* – На этапе привыкания конфликт естественен и неизбежен. Члены рабочей группы проверяют друг друга, появляется чувство границ и устанавливается доверие между ними.

•*Этап выработки норм поведения* – выработки норм поведения разрабатываются приемлемые неписанные правила и нормы поведения, которых придерживаются все сотрудники. Члены рабочей группы знают, что можно ожидать друг от друга в процессе работы.

•*Этап выполнения* – Рабочая группа готова к реализации проекта.

•*Этап роспуска* – Это этап окончания проекта или задачи, на котором рабочая группа распускается

Ре-интеграция участника проекта – процесс ввода/вывода участника проекта в/из проекта. Руководитель проекта осуществляет подготовку к ре-интеграции сотрудников после завершения проекта (проводит личные собеседования с персоналом и их линейным руководством). Задачи руководитель проекта:

- осуществлять контроль развития членов своей команды,
- обучение участников проекта,
- предоставление проектных инструкций, документацию
- ре-интеграцию новых или вернувшихся членов команды.
- По окончании проекта, осуществлять возврат участников проекта в свои подразделения или к линейному руководителю.

Участник проекта должен быть проинформирован о своей ре-интеграции. План ре-интеграции персонала – последовательный вывод персонала из проекта. Цель управления сотрудниками состоит в том, чтобы создать и поддерживать высокоэффективную рабочую группу. Навыки общения, сплоченность группы, умение разрешать конфликты и проведение эффективных совещаний могут ускорить переход к этапу выполнения. Руководителю проекта следует всегда держать эти этапы в поле зрения и стремиться к скорейшему достижению этапа выполнения.

В группу процессов исполнения входят следующие процессы:

- Руководство и управление исполнением проекта
- Обеспечение качества
- Набор команды проекта
- Развитие команды проекта
- Управление командой проекта
- Управление коммуникациями
- Осуществление закупок
- Управление вовлеченностью заинтересованных сторон

Группа процессов мониторинга и управления проектом (Monitoring & Controlling)

Регулярно оценивает прогресс проекта и осуществляет мониторинг, чтобы обнаружить отклонения от плана управления проектом, и, в случае необходимости, провести корректирующие действия для достижения целей проекта.

Контроль также предполагает определение и создание системы отчетности для предоставления информации о состоянии проекта в заданные моменты его жизненного цикла. Отчеты предназначены не только для отражения хронологии событий, но и для раннего предупреждения случаев и ситуаций, указывающих на отклонения от плана.

Мониторинг – является неотъемлемой частью и прозрачно участвует на всех этапах управления проектом. Основная задача данной фазы по проекту – проведение мониторинга состояния по выбранным метрикам на соответствие требованиям заказчика и заинтересованных сторон. Выявленные недостатки продукта устраняются на фазе выполнения проекта.

После обнаружения ситуаций, требующих внесения изменения в план работ, руководитель проекта должен задействовать механизмы внесения изменений, которые являются составными частями процесса управления проектом.

Организация эффективных совещания по проекту потребует больше времени, чем любое другое отдельно взятое задание. Целесообразно освоить навыки проведения совещаний и обеспечения их посещаемости. Для начала зададимся вопросом: нужно ли проводить совещание? Если да, то почему? Если нет, то какую форму обеспечения информированности сотрудников следует избрать? Можно ли решить эту проблему на одном заседании, с помощью письма, письменной справки, телефонного звонка? Если совещание необходимо, то следует руководствоваться следующими рекомендациями:

Подготовка

- Поставить несколько достижимых целей для совещания. •Следует быть кратким и точным при формулировке этих целей.
- Подобрать основных участников для совещания; исключить сотрудников, присутствие которых не является обязательным.
- Выбрать время и место проведения совещания, которые удовлетворяют требованиям участников.
- Подготовить повестку дня и довести ее до сведения участников до начала совещания.
- Включить в повестку дня пункты, подлежащие рассмотрению, и ожидаемые или требуемые конечные результаты.

Проведение:

- Начать вовремя.
- Поручить кому-нибудь вести протокол заседания.
- Рассмотреть повестку дня с каждым из участников до окончания совещания
- Представить участников друг другу.
- Придерживаться повестки дня. Не отклоняться от темы.
- Поблагодарить всех выступавших на совещании.

•Закончить совещание формулировкой основных принятых решений, главных конечных результатов и предоставить подробную информацию о следующем совещании.

Каким бы полным и точным не был план, всегда будут происходить события, последствия от которых невозможно предсказать и даже контролировать. Причем эти события будут происходить в самое неподходящее время (по закону подлости) и от них будет зависеть успех проекта в целом. Руководитель проекта обязан отслеживании состояния проекта, в частности состояние менеджерского треугольника:

•*Объем работ, качество* – все ли разрабатывается в соответствии с планом работ, не упущено ли что-нибудь.

•*Сроки* – соблюдаются ли сроки проекта, вез, задач

•*Деньги* – соблюдается ли запланированный бюджет, отток, приток капитала

Алгоритм работы проектного контроля:

•Установить плановые показатели

•Получить статус проекта, текущие показатели

•Сравнить план с фактом

•Установить отклонение, тенденции и степень влияния на цели проекта

•Изменить план и/или назначить меры для устранения помех ведущих к отставанию по плану.

Определение средств контроля предназначенных для того, чтобы сконцентрировать внимание на одном или нескольких основных компонентах проекта – состояние, затраты и сроки реализации. Эти средства используются по трем причинам:

•Отслеживание состояния проекта

•Обнаружение отклонений от плана

•Принятие корректирующих мер

Различают два вида контроля:

•**Оперативный контроль** – отслеживает изменения в потенциальных возможностях компании, что дает возможность оперативного реагирования с целью получения максимальной пользы для компании. Планирование включает краткосрочное и среднесрочное планирование, 1—3 года. Управление осуществляется за счет сравнения значений факта и плана.

•**Стратегический контроль** – анализирует будущие шансы компании, пути развития, возможные риски. Все это инструменты, позволяющие идти в будущее. Планирование включает долгосрочное развитие, до 10 лет.

Для любого проекта характерны отклонения от плана. При этом отклонения могут быть двух типов:

•*Позитивные отклонения* – Опережение графика или реализация проекта с меньшими затратами являются отклонениями от плана, которые звучат музыкой для руководителя проекта. Позитивные отклонения позволяют пересмотреть план и выполнить проект раньше намеченного срока или с меньшими затратами.

•*Негативные отклонения* – Отставание от графика или перерасход финансовых средств. Такая ситуация может возникнуть по причинам, которые руководитель проекта или рабочая группа не в состоянии контролировать. Независимо от причины, руководитель проекта обязан найти способы исправления ситуации. Кроме выявления причины отклонения от плана и ее ликвидации, руководитель должен найти способы переброски ресурсов с заданий, не находящихся на критическом пути, на задания, которые привели к негативному отклонению от плана. Цель – привести проект в соответствие с планом. В любом случае данные отклонения должны быть зафиксированы в периодических отчетах

по состоянию проекта.

Очень легко увлечься средствами контроля и сопутствующими им отчетами. Чем больше средств контроля взято на вооружение, тем меньше вероятность провала проекта, и наоборот, чем слабее контроль, тем выше риск обнаружить серьезные проблемы слишком поздно, чтобы их решить. Решение – компромисс в системе контроля. Частота проведения контроля так же не должна быть слишком частой. Людям надо давать время на работу, а не на постоянный сбор статистики.

В группу процессов мониторинга и управления входят следующие процессы:

- Мониторинг и управление работами проекта
- Управление изменениями и контроль изменений
- Подтверждение содержания
- Контроль и управление содержанием
- Контроль и управление расписанием
- Контроль и управление стоимостью
- Процесс контроля качества
- Мониторинг и контроль коммуникаций
- Мониторинг и контроль рисков
- Контроль закупок\исл\контрактов
- Контроль вовлеченности заинтересованных сторон

Группа завершающих процессов управления проектом (Closing)

После реализации, проект подходит к финальной стадии – завершению. Проект является завершенным с точки зрения достижения поставленных целей проекта и получения ожидаемых конечных результатов. Кроме этого владельцы проекта или руководство организации могут принять решение по досрочному завершению проекта, или изменение целей проекта приводящие к его завершению. Основанием для окончания проекта являются:

- официальное завершение работ по контрактам с поставщиками, производителями и заказчиками.
- официальное завершение заданий, выполняемых членами рабочей группы проекта
- приемка работы по проекту и конечных продуктов заказчиком;
- обеспечение получения всех конечных результатов в установленные сроки, в рамках бюджета и в соответствии с требованиями к проекту;
- надлежащее документирование проекта и предоставление базовой информации для облегчения процесса взаимодействия сотрудников или внесения изменений, которые могут потребоваться в будущем;
- выпуск и визирование окончательного отчета или отчета о состоянии проекта, которое показывает, что ожидаемые конечные результаты получены;
- прекращение всех работ по проекту как внутри организации, так и за ее пределами.

Существуют следующие три типа окончания проекта:

посредством прекращения – означает, что запланированные работы по проекту либо успешно выполнены, либо не увенчались успехом, и было принято решение об его окончании.

посредством включения – означает, что проект увенчался успехом, а его конечные продукты внедрены

посредством интеграции – самый распространенный и самый сложный способ завершения успешных проектов. Оборудование, материалы и персонал должны быть возвращены в головную организацию. В отличие от окончания проекта посредством включения, проект не может рассматриваться как конкурент при интеграции ресурсов.

В любом случае процесс завершения проекта включает в себя следующие основные стадии:

- приемка конечного продукта заказчиком,
- документирование проекта,
- проведение проверки после реализации проекта
- выпуск окончательного отчета

Следующий список может оказать помощь при определении готовности проекта к окончанию без учета опубликованных или запланированных дат и крайних сроков:

- Согласуется ли все еще проект с поставленными целями?
- Является ли он практичным? Полезным?
- Достаточно ли руководство заинтересованно в проекте, чтобы поддержать его реализацию?
- Имеет ли организация достаточно финансовых средств для реализации проекта?
- Является ли поддержка данного проекта достаточной для его успешной реализации?
- Имеет ли организация требуемую квалификацию для реализации проекта?
- Лишился ли проект ключевой фигуры или поддержки?
- Заинтересована ли рабочая группа в успехе проекта?
- Какова вероятность достижения минимума поставленных целей проекта?
- Является ли он все еще прибыльным и своевременным?

Сложность и продолжительность процесса завершения проекта определяются размером, сложностью и масштабом самого проекта. Один из важнейших вопросов по окончанию проекта – вознаграждение за успехи и извлечение уроков из неудач.

Группа завершающих процессов содержит следующие процессы:

- Заккрытие проекта или фазы (Close Project or Phase)
- Заккрытие контрактов (Close Procurement)

Завершение может состоять из:

- Тестов разработанной системы (протокол тестирования)
- Процедура сдачи-приемки, передача рабочей документации
- Аттестация персонала, извлечение уроков (Lesson Learning), обмен опытом
- Финансовый расчет и анализ фактических расходов
- Ликвидация рабочих мест и ре-интеграция персонала

Область знаний по управлению проектами (PMBooK)

Руководство PMBooK (Project Management Body of Knowledge) описывает десять областей знаний, которыми должен обладать руководитель проекта. В стандарте рассматривается каждая область знаний в отдельности, описываются её процессы входов и выходов. Процессы областей знаний представлены в PMBooK в виде дискретных элементов, которые имеют четко определенные границы. Правда на практике эти процессы являются итеративными – могут взаимодействовать между собой и накладываться друг на друга. Стандарт рассматривает следующие области знаний по управлению проектами:

Управление интеграцией проекта (Project Integration Management)

Под интеграцией понимается объединение, консолидация, сочленение и разнообразные интегративные действия, направленные на успешное управление ожиданиями заинтересованных сторон и выполнения определенных требований. Интеграция описывает распределение ресурсов по проекту, процессы поиска компромиссов, между конфликтующими целями и альтернативами, а также определяются интегральные связи между остальными областями знаний.

Управление содержанием проекта (Project Scope Management)

Под управлением содержанием понимаются процессы, позволяющие производить выборку, фильтрацию и группировку по проекту тех и только тех работ, которые понадобятся руководителю проекта для успешного завершения проекта. Управление содержанием проекта напрямую связано с определением и контролем того (содержания), что будет включено и что не будет включено в проект. Описываются схемы процессов Сбора требований, Определения содержания проекта, создания Иерархической структуры работ – ИСР (Work Breakdown Structure, WBS), Подтверждения содержания и Управления содержанием. При разработках WBS используется правило «8/80» (1 день – 2 рабочие недели). Пакет Работ (Work Breakdown Package WB) должен быть разработан за период от 8 до 80 часов. Каждый Пакет Работ должен быть назначен на конкретное подразделение или сотрудника.

Управление сроками проекта (Project Time Management)

Под управлением сроками проекта или точнее говоря временем т. к. время, более широкое понятие, понимаются процессы, посредством которых обеспечивается своевременное завершение проекта. Схема данных процессов подразумевает: Определение операций, Определение последовательности операций, Оценка ресурсов операций, Оценка длительности операций, Разработка расписания и Управление расписанием.

Управление стоимостью проекта (Project Cost Management)

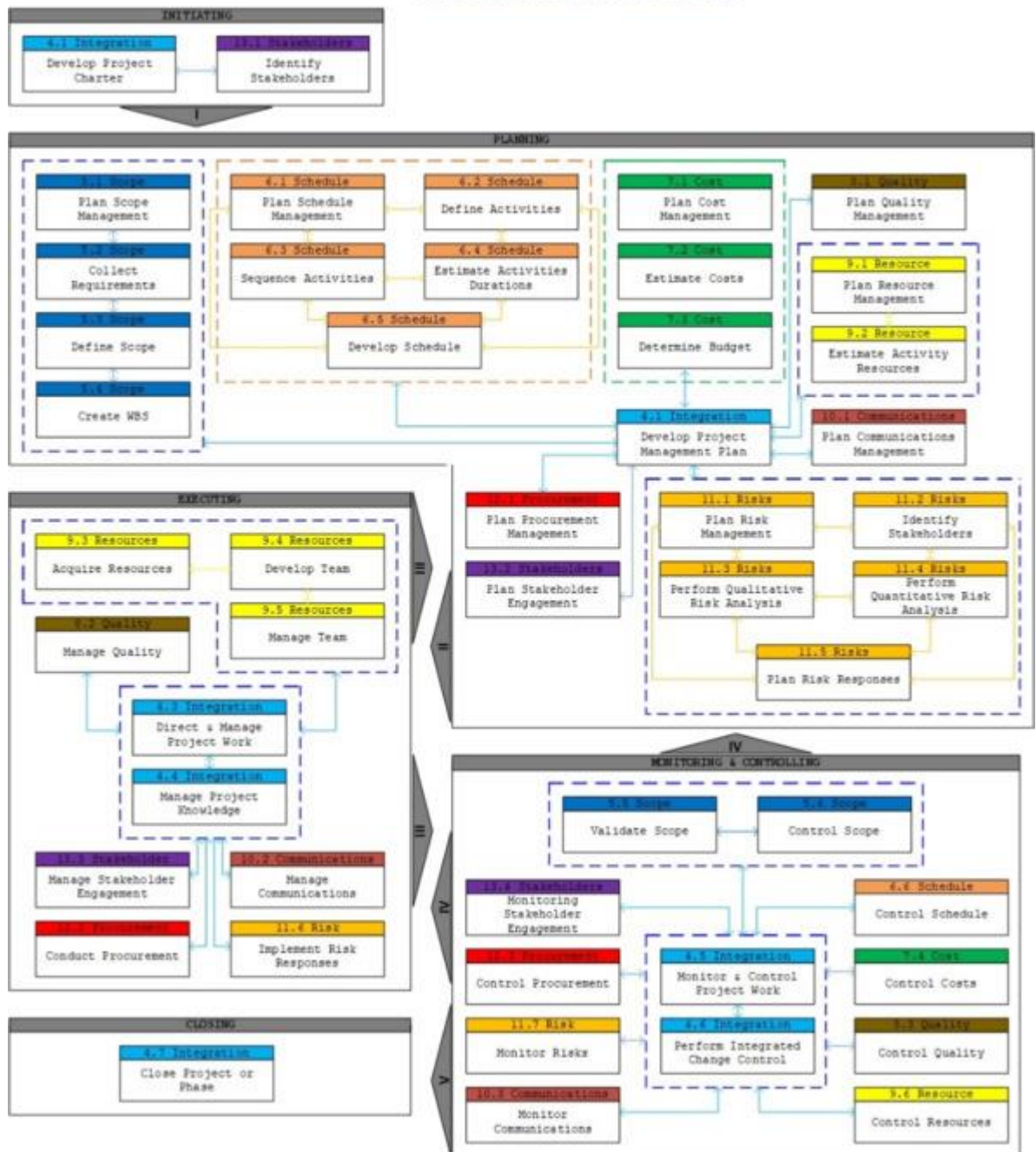
Под управлением стоимостью проекта понимаются процессы, в части планирования и разработки бюджета, а также управления расходами, которые обеспечивают завершение проекта в рамках утвержденного бюджета. Общая блок-схема процессов включает в себя: Оценку стоимости, Определения бюджета и Управление стоимостью.

Оценка – основа планирования. Рассматривая рабочие пакеты, мы оцениваем: время, персонал, издержки. Оценка – это некая величина, которая ставится на основе опыта работы с другими проектами. Для повышения степени надежности оценок можно воспользоваться следующими методами Оценки Затрат: Метод аналогий, Экспертная оценка или Метод показателей.

В качестве механизмов и техник оценки расчета стоимости проекта можно использовать: Экспертное мнение, Аналогичный проект, Параметрический, Ballpark Estimate (Rough Order of Magnitude ROM), Top-down, Three-point Estimate или Button-up метод.

Наиболее точный метод (Button-up), но при этом он требует наличие Структуру Рабочих Пакетов (Work Breakdown Structure WBS).

PMBOOK Guide v6 Processes Map



Разделение по группам процессов управления проектами и областям знаний.

Управление качеством проекта (Project Quality Management)

Под управлением качеством проекта подразумеваются процессы и различные действия со стороны исполняющей организации, подходы и политики в области качества, цели, задачи и зоны ответственности в области качества. Проект должен удовлетворять тем потребностям, ради которых он был инициирован. Само управление качеством проекта производится с помощью системы управления качеством, которая предусматривает набор определенных правил и процедур, в том числе и действия по постоянному совершенствованию процессов. Лучшей практикой считается, когда данные действия проводятся на всем протяжении проекта. Схема процессов управления качеством включает в себя: Планирование качества, Обеспечение качества и Контроль качества.

Управление человеческими ресурсами проекта (Project Human Resource Management)

Процессы управления человеческими ресурсами организации, включают в себя подходы к управлению и руководством команды проекта. Под командой проекта подразумевается пул квалифицированных работников, для которых определены конкретные роли и ответственности за выполнение проекта. В ходе реализации проекта профессиональный и количественный состав команды проекта может меняться. Правильное распределение ролей по проекту и ответственности между членами команды проекта даёт возможность всем членам команды быть задействованными на этапе планирования проекта и принятия решений. В случае привлечение членов команды к проекту на ранних стадиях даёт возможность применять имеющийся у них опыт уже на этапе планирования проекта, позволяет укрепить нацеленность команды проекта на достижение определенных результатов. Схема процессов управления человеческими ресурсами включает в себя: Разработку плана управления человеческими ресурсами, Набор команды проекта, Развитие команды проекта и Управление командой проекта.

Управление коммуникациями проекта (Project Communications Management)

Процессы управления коммуникациями, применяют с целью обеспечения своевременного формирования, подготовки, распространения, архивации, передачи, получения, использования информации на проекте. Наибольшая часть времени на проекте, у руководителей проектов уходит на осуществление коммуникаций с членами команды и с другими заинтересованными сторонами проекта. Эффективность коммуникации заключается в том, что они служат связующим звеном между различными заинтересованными сторонами, вовлеченными в конкретный проект. Правильное управление коммуникациями заключается в объединении разнообразных культурных и организационных особенностей, консолидации накопленного опыта, сопоставления различных взглядов и интересов с целью выстраивания базовой структуры управления проектом. Схема процессов управления коммуникациями проекта включает в себя:

- Определение заинтересованных сторон проекта,
- Планирование коммуникаций,
- Распространение информации,
- Управление ожиданиями заинтересованных сторон
- Отчеты об исполнении.

Движение информации распространяется по следующим каналам:

•*Руководитель проекта – проектная комиссия*, руководитель предприятия. Отчеты по проекту, расходы, анализ тренда вех и расходов, причины отклонений.

•*Проектная команда – руководитель проекта*. Команда дает отчет о проделанной работе, проблемах. Руководитель проекта дает команде информацию о дальнейших действиях и решениях, которые затрагивают их работы.

•*Пользователи, потребители продукта – руководитель проекта*. Информация о развитии проекта.

•*Руководитель проекта – план проекта*. Планы постоянно отслеживаются, т. к. это основа проектного контроллинга.

•*Проектная команда – руководители функциональных единиц*. Владелец ресурса, в случае функциональной организации компании, должен контролировать своих сотрудников с точки зрения компетенции, знаний мотивации, распределения по проектам.

Управление рисками проекта (Project Risk Management)

Под процессами управления рисками проекта понимается планирование управления рисками, идентификация и анализ рисков, выработка методов реагирования на риски, контроль, мониторинг и управление рисками в ходе реализации проекта. Посредством процессов управления рисками проекта, руководители проектов добиваются повышения вероятности возникновения и воздействия (влияния) благоприятных рисков (событий)

на проект и снижают вероятность возникновения и влияния неблагоприятных событий на проект в момент исполнения проекта. Схема процессов управления рисками проекта включает в себя:

- Планирование управления рисками,
- Идентификация рисков,
- Качественный анализ рисков,
- Количественный анализ рисков,
- Планирование реагирования на известные риски,
- Мониторинг и управление рисками.

Управление поставками проекта (Project Procurement Management)

Процессы управления поставками проекта включают в себя покупку или приобретение тех или иных необходимых сущностей (продукты, услуги, результаты, документы), которые производятся внешними организациями по отношению к той, в которой реализуется проект. Сама организация, в которой выполняется проект может выступать в качестве покупателя или продавца этих сущностей. Также процессы управления поставками проекта включают в себя под-процессы управления контрактами и изменениями, необходимые для разработки и сопровождения контрактов или заказов на покупку. Благодаря процессам управления поставками проекта появляется возможность администрировать все контракты на приобретение чего-либо в ходе реализации проекта и управлять контрактными обязательствами, которые были возложены на команду проекта. Схема процессов управления поставками проекта включает в себя:

- Планирование закупок,
- Осуществление закупок,
- Управление закупочной деятельностью,
- Закрытие закупок.

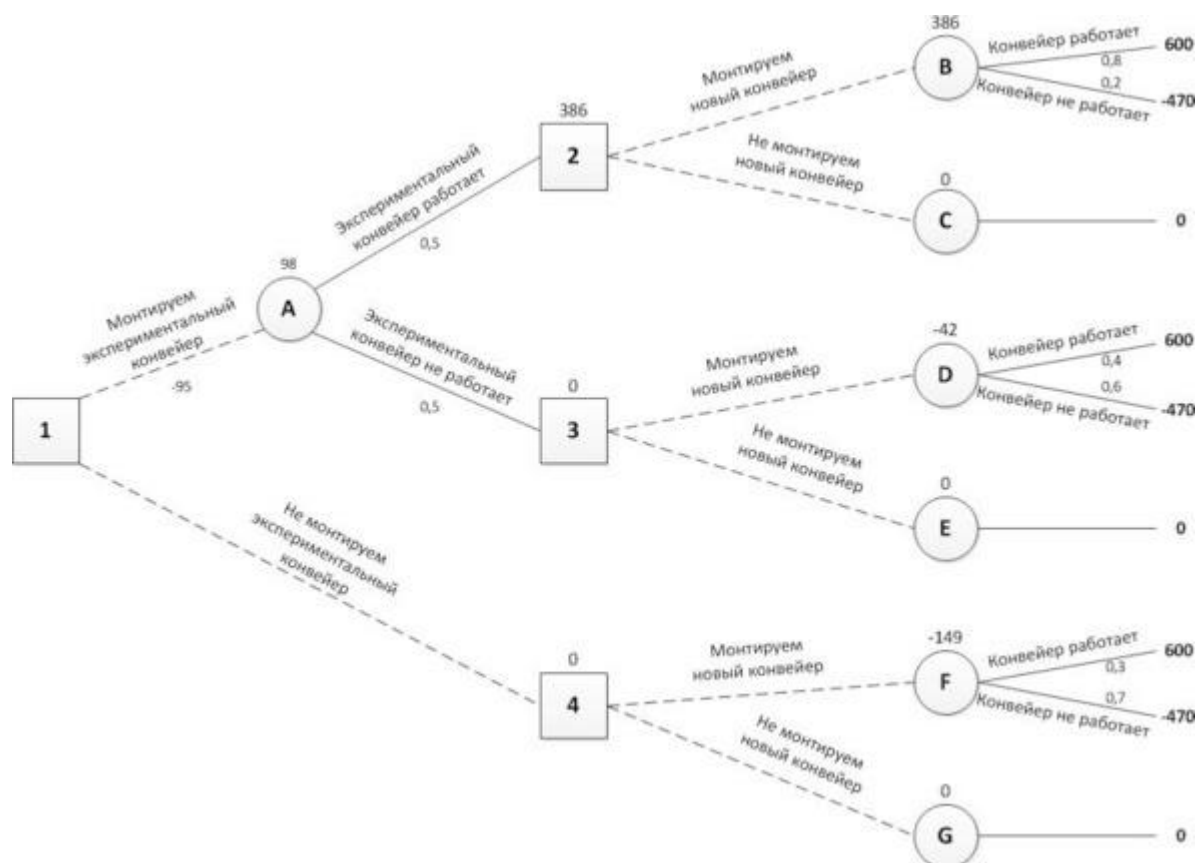
Управление заинтересованными сторонами проекта (Project Stakeholder Management)

Под процессами управления ожиданиями заинтересованными сторонами проекта понимается как таковое общение между командой проекта и заинтересованными лицами, а также работы, направленные на удовлетворение их потребностей и решение возникающих проблем, которые могут повлечь за собой изменения на проекте. Благодаря правильному выстраиванию отношений между всеми заинтересованными сторонами на проекте, Руководитель проекта может увеличить вероятность успеха.

Методы и техники Управления Проектами

В методологии PMI описываются различные инструменты и техники, применяя которые на практике, руководитель проекта может повысить эффективность исполнения проекта, предусмотреть риски, высчитать оптимальные маршруты прохождения проекта, здраво оценить ситуацию и изначально принять правильное решение и т. д. Данные инструменты и техники существуют сами по себе и уже давно применяются в различные направления деятельности человека. Ниже приведен список основных методов и техник применимых к определенным процессам.

Анализ дерева решений (Decision Tree Analysis)



Анализ дерева решений (Decision Tree Analysis).

Анализ дерева решений (Decision Tree Analysis) – это метод, который описывает процесс принятия решения посредством рассмотрения альтернативных вариантов и последствий их выбора. Этот метод используют в тех случаях, когда прогнозируемые сценарии и результаты действий, имеют вероятностный характер. Отображается в виде диаграммы. В диаграмме анализа дерева решений отражаются вероятности и величины затрат, выгоды каждой логической цепи событий и будущих решений, и используется анализ ожидаемого денежного значения с целью определения относительной стоимости альтернативных действий.

При формировании дерева используются четыре следующих типа графических обозначений:

- Квадраты – места принятия решений.
- Круги – места появления исходов.
- Пунктирные линии – возможные решения.
- Треугольники или прямые линии – возможные исходы.

Необходимо рассчитать ожидаемую стоимостную оценку (EMV) для каждой альтернативы – максимальную состоящую из сумм оценок выигрышей, которые необходимо умножить на вероятность реализации выигрышей, для всех возможных вариантов.

Анализ сильных и слабых сторон, возможностей и угроз (SWOT Analysis)

SWOT-анализ (Strengths Weakness Opportunities Threats Analysis) – это метод оценки внутренних и внешних факторов, которые влияют на развитие компании. Он поможет вам оценить сильные и слабые стороны вашего дела, найти новые возможности и определить возможные угрозы. SWOT-анализ разделяет факторы влияния на компанию на четыре категории, что помогает оценить её со всех сторон, это:

S-strengths (сильные стороны) . Например, продажа товаров непосредственно покупателю, прибыль больше, чем у конкурентов, клиент-сервис – лучший на рынке и т. д.;

W-weaknesses (слабые стороны). Например, недостаточно партнёров, неэффективная реклама, маленькая целевая аудитория;

O-opportunities (возможности). Например, потенциальные клиенты узнают всё, что им нужно о вашем товаре из Интернета, покупки совершаются круглосуточно, не зависимо от того, работаете вы или нет;

T-threats (угрозы). Например, бренд ваших конкурентов более известный на рынке, качество товаров, которые предлагают конкуренты выше.

SWOT-анализ часто используют при стратегическом планировании. С него может начинаться любое действие компании. Например, такие как исследование новых инициатив, новые стратегии развития, возможные изменения.

Внутренние факторы – сильные и слабые стороны относятся к внутренним факторам, а значит, вы их легко можете оценить:

- Финансовые ресурсы. Это финансирование, возможности получения дохода;
- Физические ресурсы. Это ваше оборудование, здания, местоположение;
- Человеческие ресурсы. Сотрудники, иногда волонтеры, целевая аудитория;
- Доступ к природным ресурсам, авторские права, патенты;
- Текущие процессы. Сюда относится всё, что происходит в компании, мотивационные программы, программы обучения, система иерархии отделов и т. д.

Чтобы найти сильные стороны своего бизнеса ответьте на такие вопросы:

- Какие преимущества у вашего бизнеса?
- Что вы делаете лучше, чем все остальные?
- Какие ваши сильные стороны видят ваши клиенты?
- Какое у вас уникальное торговое предложение (УТП)?
- Как вы можете увеличить свою прибыль?

Рассмотрите свои сильные стороны, как с внутренней точки зрения, так и с точки зрения ваших клиентов. Оценивайте свои сильные стороны относительно к конкурентам.

Внешние факторы – Влияние внешних обстоятельств на каждую организацию и отдельного человека очень сильное. Внешние факторы – это, как правило, те обстоятельства, которые вы и ваша компания не может контролировать:

- Рыночные течения. Сюда можно отнести новые продукты, технологии, изменения потребностей целевой аудитории;
- Экономические тенденции. Это местные, национальные, международные финансовые направления;
- Финансирование. Такие, как пожертвования, государственные влияния, налоги и т. д.;
- Демографические данные. Это возраст, пол, раса, национальность, культурные ценности целевой аудитории;
- Отношения с поставщиками и партнёрами;
- Политическая, экологическая, экономическая ситуация в стране.

Метод оценки и анализа программ (Program Evaluation and Review Technique, PERT)

Метод PERT (Program Evaluation Review Technique PERT), Техника Оценки и Анализа Программ и проектов часто используется при управлении проектами и проведении анализа производственных процессов. Метод PERT является инструментом, который вычисляет ожидаемое значение продолжительности проекта или отдельного процесса. При управлении проектами метод PERT практически всегда используется в сочетании с методом критического пути (англ. CPM, Critical Path Method).

Метод PERT и метод критического пути принципиально различаются по области их применения. Метод критического пути используется для оценки сроков завершения всего

проекта или групп взаимосвязанных задач, а метод PERT применяют для оценки длительности отдельных задачи. Сама идея метода крайне проста – для того, чтобы оценить время выполнения задачи или процесса, вам необходимо знать оптимистичную, пессимистичную и наиболее вероятную оценку продолжительности этой задачи. Формула PERT выглядит следующим образом:

$$E = \frac{(O + 4M + P)}{6}$$

О – оптимистичная оценка длительности задачи,

М – наиболее вероятная оценка длительности задачи,

Р – пессимистичная оценка длительности задачи.

Это уравнение представляет собой ни что иное, как средневзвешенное значение, где, наиболее вероятная оценка длительности имеет вес 4 раза больший, чем оптимистична и пессимистичная оценки. Такой подход предотвращает слишком сильный перекося в одном из направлений.

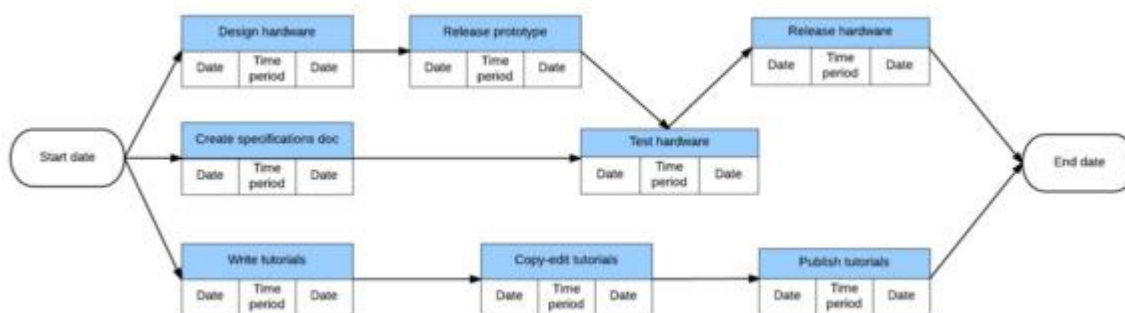
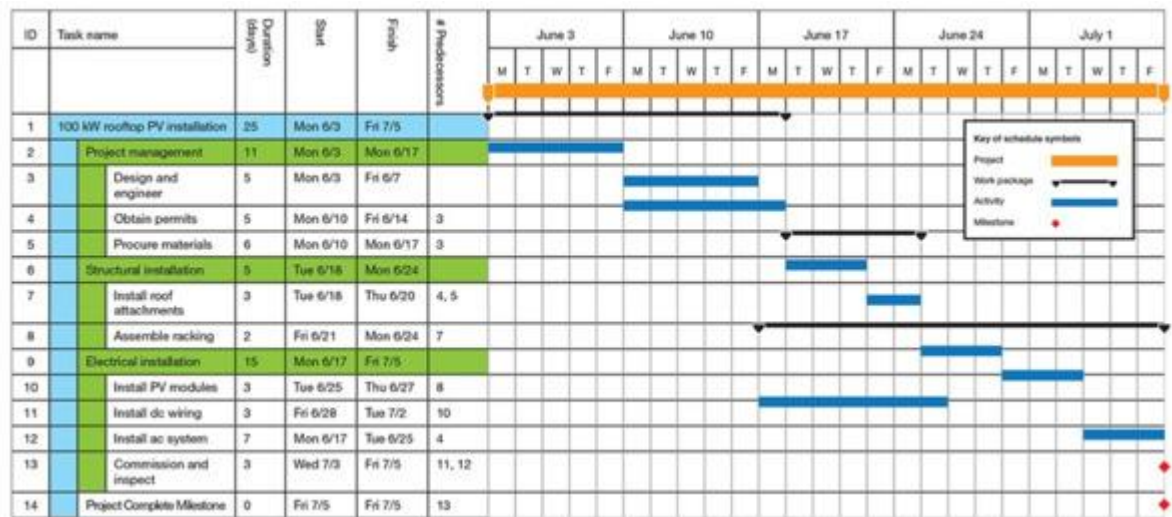


Диаграмма «PERT Chart»

Диаграмма Гантта (Gantt Chart)

Диаграмма Гантта (также ленточная диаграмма, график Гантта) – это популярный тип столбчатых диаграмм (гистограмм), который используется для иллюстрации плана, графика работ по какому-либо проекту. Является одним из методов планирования проектов. Используется в приложениях по управлению проектами. В настоящее время диаграмма Гантта является стандартом де-факто в теории и практике управления проектами, по крайней мере, для отображения структуры перечня работ по проекту.

Диаграмма Гантта представляет собой отрезки, размещенные на горизонтальной шкале времени. Каждый отрезок соответствует отдельному проекту, задаче или подзадаче. Проекты, задачи и подзадачи, составляющие план, размещаются по вертикали.



Начало, конец и длина отрезка на шкале времени соответствуют началу, концу и длительности задачи.

Анализ освоенного объема (EVA)

Анализ освоенного объема (EVA) – это расчет показателей эффективности проекта в рамках освоенного объема. EVA основывается на тех же принципах, что и анализ тренда расходов и используется как правило в крупных проектах. За основу берутся цифры: Освоенный объем, плановые и фактические расходы. Рассмотрим на примере:

Задачу (ЗП1) должен выполнить один исполнитель (ИС1). Выделено по плану – два дня (2 x 8 часов = 16 часов) времени, стоимость работ исполнителя \$ 10.00 в час (плановый расход = \$ 10.00 x 16 часов = \$ 160.00).

По факту: исполнитель закончил работу на третий день, дополнительно истратив два часа, сверх запланированных. Показатели: Факт по времени (2 x 8 часов + 2 часа = 18 часов), и фактические расходы = \$ 10.00 x 18 часов = \$ 180.00.

Результат:

На утро третьего дня: результат выполнения задачи ЗП1 = $16 / (16 + 2) * 100\% = 89\%$ и стоимость выполнения ЗП1 = \$ 180.00

Вывод: Здравый смысл говорит нам о том, что мы тратим деньги быстрее, чем получаем результат.

Основные показатели метода:

Плановый объем (Planned Value PV) – объем запланированных работ в базовых ценах. Или другое название – БСЗР (базовая стоимость запланированных работ). В нашем примере PV равен 160\$, т. к. базовый объем работ, который должен быть выполнен к среде, равен 16 чел-часам, а базовая цена равна 10\$ за час работы.

Освоенный Объем (Earned Value EV) – выполненная часть работ от запланированного объема. Измеряется как % завершения работы, умноженный на базовый бюджет задачи. Ранее этот показатель назывался БСВР (базовая стоимость выполненных работ). В нашем примере EV равен 142\$, т. к. % выполнения по задаче равен 89%, а ее базовый бюджет составляет 160\$.

Фактическая стоимость (Actual Cost AC) – реальная стоимость выполненных работ. Измеряется количеством денег, которые мы по факту уже должны за выполненную работу. В нашем примере AC равен 160\$, т. к. фактически исполнитель затратил 16 часов, а каждый час стоит 10\$.

Бюджет по завершению БПЗ (Budget At Completion BAC) фиксируется на старте проекта как сумма утвержденного бюджета на весь проект. В нашем кейсе он равен 160\$.

Отклонение по стоимости (Cost Variance CV) – отклонение по стоимости (формула:

$CV=EV-AC$). $\$ 142.00 - \$ 160.00 = - \$ 18.00$. Отрицательное значение – превысили бюджет, положительное – экономим бюджет. В нашем случае – Мы перерасходовали бюджет.

Отклонение от календарного плана ОКП (Schedule Variance SV) – отклонение по срокам (формула: $SV=EV-PV$). $\$ 142.00 - \$ 160.00 = - \$ 18.00$. Отрицательное значение – отстаем от плановых сроков, положительное – опережаем сроки. Мы отстаем от графика.

Индекс отклонения по стоимости ИОС (Cost Performance Index CPI) – индекс выполнения стоимости (формула: $CPI=EV/AC$). Индекс больше 1 – идем с экономией бюджета, меньше 1 – превышаем бюджет. В нашем случае $\$ 142.00 / \$ 160.00 = 0,89$. Перерасход бюджета по задаче на 11%

Индекс отклонения от календарного плана ИОКП (Schedule Performance Index SPI) – индекс выполнения сроков

(формула: $SPI=EV/PV$). Индекс больше 1 – опережаем график работ, меньше 1 – отстаем от базового графика.

В нашем случае: $SPI = \$ 142.00 / \$ 160.00 = 0,89$. Отстаем по срокам задачи на 11%

Предварительная оценка по завершению ПОПЗ (Estimate At Completion EAC) – Представляет ожидаемую общую стоимость проекта после завершения оставшихся работ (Формула: $EAC=BAC/CPI$). В нашем случае: $\$ 160.00 / 0,89 = \$ 180.00$. На сегодняшний день оценочная стоимость задачи проекта = $\$ 180.00$.

Оценка до завершения ОДЗ (Estimate To Complete ETC) – Сколько еще нужно денег, чтобы завершить проект (Формула: $ETC=EAC-AC$). В нашем случае: $ETC=EAC-AC=\$ 180.00 - \$ 160.00 = \$ 20.00$ – еще нужно на сегодняшний день, чтобы завершить задачу.

Отклонение бюджета по завершению ОБЗ (Variance At Completion VAC) – Ожидания по перерасходу или экономии бюджета (формула: $VAC = BAC-EAC$). В нашем случае: $VAC = BAC-EAC = \$ 160.00 - \$ 180.00 = - \$ 20.00$. На 20\$ мы перерасходуем бюджет.

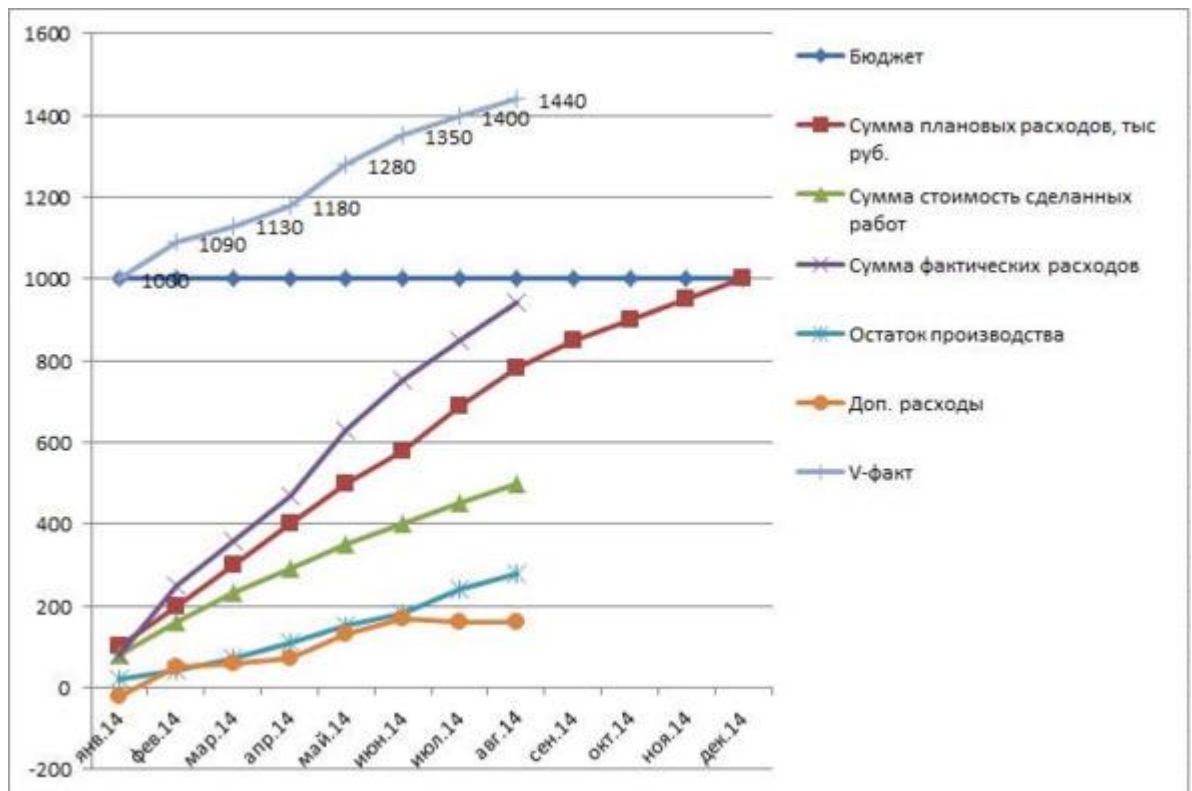
Формулы для расчета состояния проекта: $EAC = AC + Button-up ETC$, $EAC = AC + BAC - EV$, $EAC = BAC / Cumulative CPI$, $EAC = AC + [(BAC - EV) / Cumulative CPI \times Cumulative SPI]$, $EMV = probability \times impact$, $EV = BAC / \% \text{ of completion}$, $TCPI = (BAC - EV) / (BAC - AC)$,

Анализ тренда расходов

Анализ тренда расходов – это метод наблюдения за проектом, за распределением его расходов. Предназначен для выравнивания бюджета по вехам, проекту в целом и своевременным контролем скачков затрат.

Постоянно контролируемые значения:

- Плановые расходы – то, что было запланировано изначально на реализацию.
- Фактические расходы – то, что было затрачено по факту на сделанную работу.
- Стоимость сделанных работ – то, что было запланировано и в действительности потрачено на сделанную работу. Сюда входит стоимость работ, материалов, внешних услуг.
- Остаток производства – то, что осталось сделать. Вычисляется как разница между запланированным объемом работы и сделанные к определенной точке во времени. Остаток производства = плановые расходы – стоимость сделанных работ.
- Дополнительные расходы – это разница между фактическими расходами и плановыми.
- Дополнительные расходы = фактические расходы – плановые расходы.



V-факт – предварительные фактические расходы. Выступает, как сигнал пере-расходования средств.

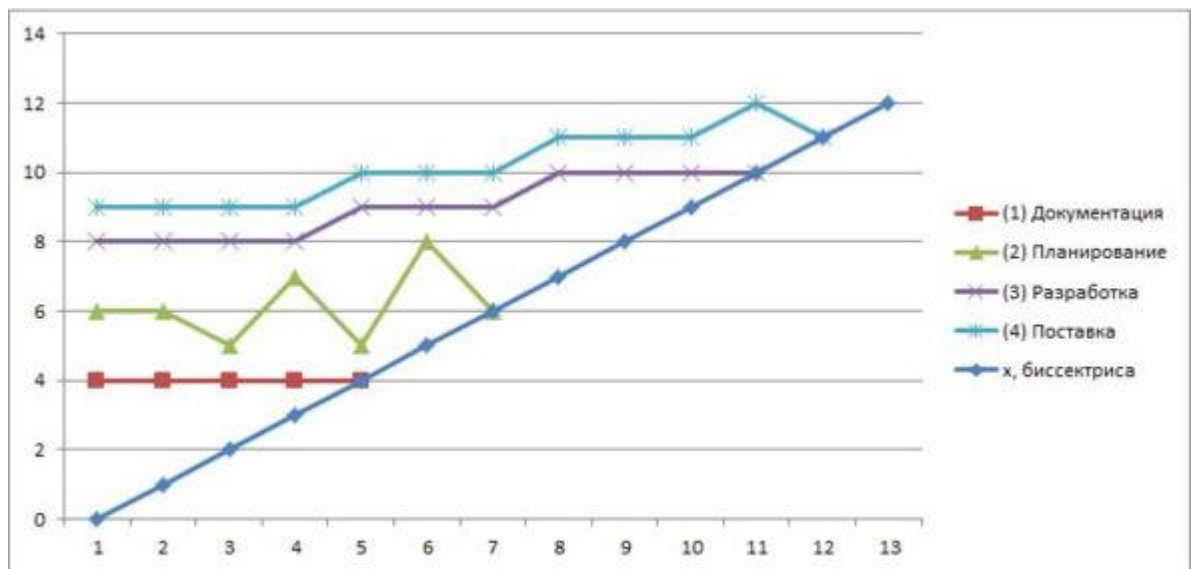
$V\text{-факт} = \text{бюджет} + \text{дополнительные расходы} + \text{остаток производства}$.

Анализ тренда этапов проекта (вех проекта)

Анализ тренда этапов проекта (вех проекта) – это метод наблюдения за проектом, за его временным отставанием или опережением. Метод позволяет обнаружить отклонения на ранних стадиях и принять соответствующие меры по улучшению ситуации. Метод построен на анализе состояния вех, текущее и запланированное. Каждая веха имеет установленный срок выполнения, запланированный на этапе планирования проекта. Это время и есть отправная точка регулярной сверки. По завершению вехи ответственные отчитывается руководителю проекта о проделанной работе. В отчете должны быть ответы на следующие вопросы:

- Что сделано?
- Что нужно еще сделать для завершения вехи?
- Успели ли в срок?

Наиболее часто для визуализации используют графическое отображение анализа тренда вех.



По горизонтали: периоды предоставления отчетности, например, каждую неделю.

По вертикале: такая же шкала, с отметками вех. Отметка вех при $X=0$, соответствует запланированным показателям вех на этапе старта проекта.

Биссектриса – обозначает положение достигнутых вех.

В отчетный период диаграмма обновляется и анализируется. На диаграмму заносятся новые прогнозные сроки по завершению вех. Для каждой вехи получаем линию (кривую) тренда. Достигла биссектрисы, закончилась.

Идеальное состояние, когда линия четко идет без изменений по оси Y.

Отклонения по вертикале (отклонение прогнозируемого срока от первоначально запланированного):

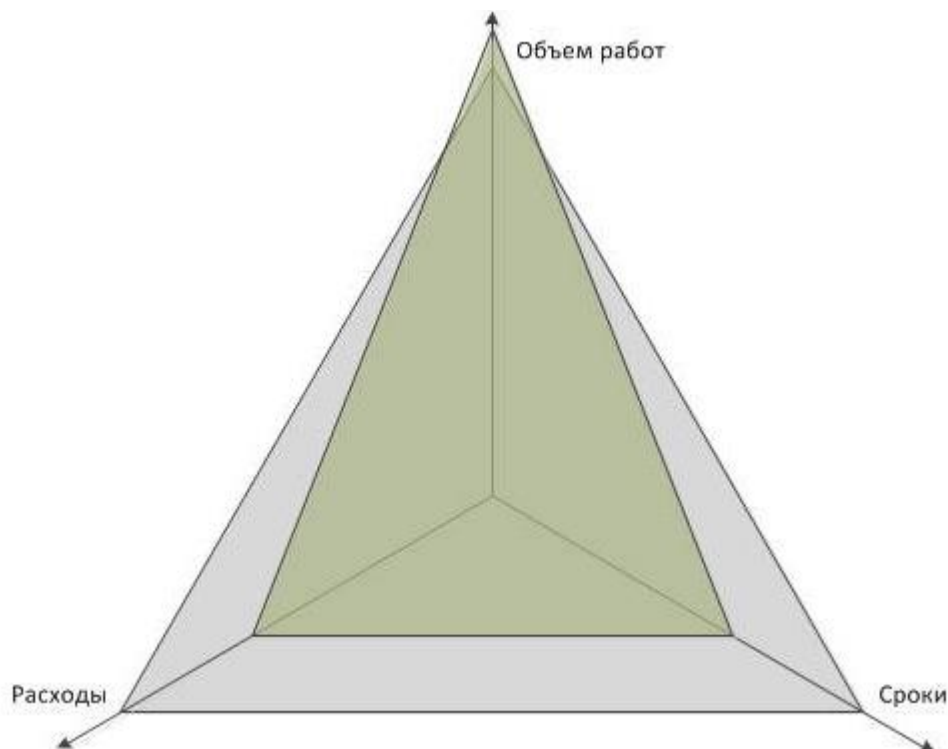
Вверх: отставание по срокам

Вниз: опережение графика

Анализ с помощью Треугольника целей

Анализ с помощью Треугольника целей – Углы треугольника обозначаются, как:

- Сроки. Время на реализацию проекта.
- Расходы. Деньги, люди, бюджет.
- Объем работ. Цели, задачи, качество.



Пример хорошего развития проекта – Объем работ соблюден и даже превышен при меньших расходах и сроках.

Равносторонний треугольник с равными сторонами показывает плановые величины для: бюджета, срока, объема работ. Картинка меняется в зависимости от отклонения от базовых плановых значений.

Результаты проекта меряются с определенной периодичностью.

Сроки – измеряется затраченным временем на проект.

Расходы – измеряются фактическими затратами.

Объем работ – измеряется в процентном соотношении запланированных и выполненных работ.

Измеренные величины на отчетную дату наносят на оси координат и получают новый треугольник, который отличается от первоначального равностороннего треугольника. Треугольник целей хорошо подходит для демонстрации, как промежуточных, так и в целом, результатов проекта.

Прочие Методы и Техники

Анализ допущений (Assumptions Analysis)

метод, посредством которого производится анализ точности допущений и идентификация рисков на проекте, вызванных неточностью, неполнотой или противоречивостью допущений. Любой проект и любой определенный риск проекта инициируется и исполняется на основании ряда гипотез, сценариев и допущений. Анализ допущений исследует обоснованность допущений применительно к проекту. Данный анализ позволяет идентифицировать риски проекта, возникающие вследствие неточности, нестабильности, противоречивости или неполноты допущений.

Анализ ожидаемого денежного значения (Expected Monetary Value Analysis EMV)

Статистический метод, вычисляющий средний результат, когда в будущем имеются сценарии, которые могут произойти, а могут и не произойти. Обычно этот метод используется в рамках анализа дерева решений.

Анализ отклонений (Variance Analysis)

Метод разложения общего отклонения совокупности переменных содержания, стоимости и расписания на отклонения отдельных элементов, которые связаны с определенными факторами, влияющими на переменные содержания, стоимости и расписания.

Анализ сети (Schedule Network Analysis или Network Analysis)

Анализ сети расписания (Schedule Network Analysis) – Метод определения ранних и поздних стартов и ранних и поздних финишей для невыполненных плановых операций проекта. См. также метод критического пути, метод критической цепи, анализ возможных сценариев и выравнивание ресурсов.

Анализ тенденций (Trend Analysis)

Аналитический метод, использующий математические модели для прогнозирования результатов в будущем на основании исторических данных. С помощью этого метода определяется отклонение от базового плана по затратам, срокам или содержанию с использованием данных из предыдущих периодов отчетности и прогнозирования величины отклонения данного параметра в определенный момент в будущем, если в исполнение проекта не будут вноситься изменения.

Анализ резервов (Reserve Analysis)

Методы анализа, служащие для определения существенных характеристик и взаимосвязей элементов в плане управления проектом с целью установления резерва для длительности расписания, бюджета, оценочной стоимости или средств проекта.

Анализ чувствительности (Sensitivity Analysis)

Метод количественного анализа рисков и моделирования, используемый для определения рисков с наибольшим возможным воздействием на проект. В процессе анализа устанавливается, в какой степени неопределенность каждого элемента проекта отражается на исследуемой цели проекта, если остальные неопределенные элементы принимают базовые значения. Обычно отображение результатов представлено в виде диаграммы «торнадо».

Быстрый проход (Fast Tracking)

Особый метод сжатия расписания проекта, изменяющий логику сети путем наложения друг на друга фаз, которые в обычной ситуации выполнялись бы последовательно, например, фазы проектирования и фазы строительства, или для параллельного выполнения запланированных операций. См. также сжатие расписания.

Выравнивание ресурсов (Resources Leveling)

метод оптимизации нагрузки ресурсов проекта путем организации оптимального выполнения работ по проекту, учитывая их приоритетность, сроки выполнения и ограничения ресурсов.

Декомпозиция (Decomposition)

Метод, предполагающий разбиение содержания проекта и результатов поставки проекта на более мелкие и легко управляемые элементы до тех пор, пока работы по проекту, связанные с выполнением содержания проекта и обеспечением результатов поставки, не определены достаточно подробно для исполнения, отслеживания и мониторинга этих работ.

Метод «операции в узлах» или метод предшествования (Precedence Diagramming

Method, PDM)

Метод составления сетевых диаграмм, в которых плановые операции представляются прямоугольниками (или узлами). Плановые операции графически связаны одной или несколькими логическими взаимосвязями, которые показывают последовательность выполнения операций.

Метод сетевых графиков

Общая группа визуального отображения в виде графиков. Сетевой график, в отличие от диаграммы Ганта графически отображает зависимости между работами, а также продолжительность каждой работы и ресурсы. После этого определяется, какие задачи являются критическими, а какие – нет. два вида сетевых графиков: Сетевой график по методу критического пути (CPM) и Сетевой график по методу потенциалов (MPM).

Метод критического пути (Critical Path Method, CPM)

пошаговая методика (сетевых графиков), используемая при реализации взаимозависимых задач. Составляется перечень работ, определяются структура их декомпозиции, временная шкала, зависимости, реперные точки и результаты. Критические и некритические работы выделяются путем расчета наибольшего (на критическом пути) и наименьшего (плавающего) времени выполнения различных задач.

Метод критического пути – довольно часто используется в строительстве и характеризуется наличием четко выраженного пути проекта, этот путь формируют самые длинные работы проекта. Сам критический путь и определяет продолжительность всего проекта. Определяя и идентифицируя наиболее важные задачи, Вы можете оценить даты завершения, зависимости, ключевые вехи и конечные результаты. Любые отставания по датам для тех работ, которые лежат на критическом пути ведут к увеличению длительности последующих работ. При необходимости сократить длительность проекта необходимо сокращать сроки работ на «критике». Методология управления проектами при помощи критического пути позволяет сравнивать плановые и фактические показатели (как ситуация должна развиваться и что происходит на самом деле) каждый день. Четыре этапа планирования по методу:

- цели и ограничения (рассмотрение проекта по нескольким аспектам – длительность, рас, качество и проч.);
- продолжительность работы;
- сетевой график работ;
- построение диаграммы Ганта

Метод критической цепи. Метод критической цепи (Critical Chain Method CCM)

отличается от метода критического пути тем, что он ориентирован на использование ресурсов проекта, а не проектных работ. Для решения потенциальных проблем с ресурсами формируются буферы, гарантирующие своевременную реализацию проектов с соблюдением всех необходимых мер безопасности. Управление проектом по методу критической цепи помогает избегать отставаний и задержек в проекте, определяя критический путь работ, а также резервы ресурсов (запас времени) для этих работ. Поскольку графики строятся, учитывая доступность ресурсов, срок проекта может быть дольше, но вероятность срыва сроков ключевых событий может быть снижена. Основа методологии критических цепочек – формирование основных работ критически важных для проекта и удержание сроков работ, соответственно и финальной даты завершения проекта. Критические работы проекта провязываются логическими связями с учетом ресурсных и административных ограничений; Если в проекте ресурсы не ограничены, расчётные показатели будут схожими с PERT. Если в проекте все же ограничены ресурсы, то необходимо:

- Определить околоскритические работы в графике, такие работы очень часто идут параллельно основной «красной»

•цепочки, но с уменьшенными сроками, они могут довольно легко стать критическими если им не уделять внимание.

•Определить критическую цепочку проекта при помощи ресурсных связей

Метод Монте-Карло (Monte Carlo Analysis)

Метод, многократно рассчитывающий (или выполняющий итерации) стоимости проекта или длительности проекта с использованием входных величин, произвольно взятых из возможных значений стоимости или длительности, с целью получения распределения вероятностей значения общей стоимости проекта или дат завершения проекта.

Метод оптимизации выгод (Value Engineering, VE)

Творческий подход к оптимизации стоимости на этапах жизненного цикла проекта, сокращению временных затрат, увеличению прибыли, улучшению качества, расширению рынка сбыта, разрешению проблем и/или повышению эффективности использования ресурсов.

Метод освоенного объема (Earned Value Technique, EVT)

Особый метод для измерения исполнения работ для элемента иерархической структуры работ, контрольного счета или проекта. Другое название – «метод правил освоения и начисления дохода» (earning rules and crediting method).

Оценка «снизу-вверх» (Bottom-up Estimating)

Метод оценки элемента работ. Работа разбивается на более мелкие работы. Подготавливается оценка того, что нужно для выполнения требований каждой из частей работы, и эти оценки затем суммируются для данного элемента работ. Точность оценки «снизу-вверх» определяется размером и сложностью работ, выделенных на более нижних уровнях. Обычно меньшее содержание работ увеличивает точность оценок.

Оценка «Сверху вниз» (Top-down Estimating)

Метод оценки элемента работ. Обратный методу «снизу-вверх».

Планирование методом набегающей волны (Rolling Wave Planning)

Вид планирования последовательной разработки, при котором работа, которую надо будет выполнить в ближайшей перспективе, подробно планируется с глубоким раскрытием иерархической структуры работ, в то время как далекая работа планируется с относительно неглубоким раскрытием иерархической структуры работ, но по мере выполнения работ производится подробное планирование работ, которые надо будет выполнить в ближайшие временные периоды.

Управление освоенным объемом (Earned Value Management, EVM)

это методология управления для интеграции содержания, сроков и ресурсов, а также объективного измерения исполнения проекта и достигнутой эффективности. Эффективность исполнения проекта измеряется путем определения плановой стоимости выполненных работ (т. е. освоенного объема) и ее последующего сравнения с фактической стоимостью выполненных работ (т. е. фактической стоимостью).

Иерархическая структура рисков (Risk Breakdown Structure, RBS)

Иерархически организованное представление известных рисков проекта, распределенных по категориям и подкатегориям риска, указывающим различные области и причины возможных рисков. Иерархическая структура рисков часто подгоняется под конкретные типы проектов.

Матрица вероятности и последствий (Probability and Impact Matrix)

Общепринятый подход для отнесения риска к высоким, средним или низким путем сопоставления двух параметров риска: вероятности и воздействия на цели проекта в случае его наступления.

Матрица ответственности (Responsibility Assignment Matrix, RAM)

Структура, ставящая в соответствие организационную структуру иерархической структуре работ и помогающая назначению лиц, ответственных за каждый элемент содержания проекта.

Расписание контрольных событий (Milestone Schedule)

Укрупненное расписание работ, отображающее сроки наступления основных контрольных событий.

Метод аналогий

Сущность метода аналогий состоит в анализе всех имеющихся данных, касающихся осуществления фирмой аналогичных проектов в прошлом, с целью расчета вероятностей возникновения потерь. Техника предполагает следующие ключевые аспекты действий: Попытка сравнить с аналогичным проектом, выполненным ранее. Собирается информация по планируемому и фактическому сроку выполнения, если сроки не совпадали, то анализируются причины приведшие к этому, вырабатываются контрмеры и формируется план проекта. Наибольшее применение метод аналогий находит при оценке риска часто повторяющихся проектов, например, в строительстве.

Метод Экспертной Оценки (Expert Judgment)

Суждения, предоставляемые на основании компетенции в области приложения, области знаний, дисциплине, индустрии и т. д., соответствующих выполняемой операции. Анализ проводится с применением различных методов с фокусом на различные аспекты. Экспертизу могут осуществлять как группы, так и отдельные лица, обладающие специализированным образованием, знанием, навыками, опытом или обучением. Может быть несколько источников, в том числе: другие подразделения исполняющей организации; консультанты; участники проекта, включая заказчиков, профессиональные и технические ассоциации и отраслевые группы.

Метод показателей

Используются показатели по завершенным проектам. Например, метод процентных ставок. При этом методе происходит полноценное распределение затрат по разным фазам. Например, если известны реальные затраты на первую фазу, то остальные вычисляются согласно процентному распределению. Пример:

- Фаза анализа – 20%
- Фаза проекта – 35%
- Фаза реализации – 30%
- Фаза тестирования – 15%

Оценка «Навскидку» Poker Estimate

Техника предполагает следующие ключевые аспекты действий:

- Собирается рабочая группа (разработчики, аналитики, представители бизнеса и т.п.).
- Озвучивается задача,
- Каждый участник оценивает сроки проекта основываясь на своем опыте и уровню,
- Каждый участник высказывает свое мнение.
- Для обсуждения рабочей группой выбираются самый короткий и самый длинный срок проекта.

•В процессе обсуждения проводится корреляция мнений после чего рабочая группа приходит к общему решению.

Оценка времени или часов разработки

Важным элементом, при ведении ИТ проекта по разработке программного обеспечения является оценка времени, необходимого для разработки продукта. Данный вопрос актуален, как при разработке решения внутренними ресурсами, так и при аутсорсинге. Классическим примером, показан на диаграмме.

Все это может привести к следующим плачевным последствиям: Срыв сроков проекта, Превышение стоимости проекта (овертаймы и т.п.) или неудовлетворенность заказчика качеством продукта.

Для устранения данных проблем можно воспользоваться следующими методами и техниками:

- Poker Estimate,
- Сравнение с аналогом,
- Bottom up & Top down
- Экспертная оценка.

После проведения анализа по одним из методик, рекомендуется добавить к срокам проекта:

- 15—20% процентов времени для покрытия рисков и непредвиденных случаев
- Принимаем в расчеты 80% процентов рабочего времени (а не 100% формальных) разработчика, как основной рабочей единицы занятой на проекте

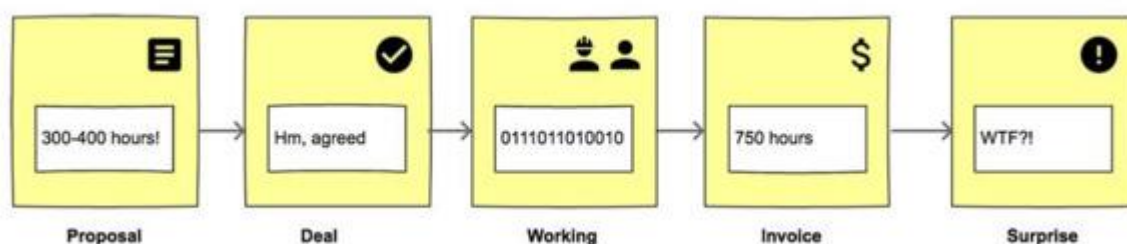


Диаграмма: Стоимость проекта

Ведение документации по проекту

Документация проекта – это набор документов, описывающих проект и регламентирующих деятельность в рамках проекта.

Проекты живут за счет быстрого обмена информации внутри проектной команды и внешними заинтересованными сторонами, поставщиками. Каждый участник проекта отвечает за предоставление или не предоставление информации.

Правило: «информация – это долг, который одни должны отдать, а другие потребовать».

Ход проектных работ должен постоянно документироваться, являясь внутренней информацией проекта. Информацию можно разделить на две части:

- Внутренняя
- Внешняя.

Внутри команды информацией по проекту могут обладать почти все участники проекта, а во вне отдается только часть информации. Пример внутренней информации:

- Планы

- Статусы
 - Протоколы совещаний
 - Документация по дефектам, тестам
 - Договоры с поставщиками
- Анализ рисков

Пример информации, которую можно отдать во вне:

- Матрица компетенций
- Журнал распределения обязанностей
- Статусы проекта
- График вех
- Заключительные отчеты

Проект документируется на протяжении всего жизненного цикла. При отсутствии регламентирующих правил работы с документами и по мере накопления документов в проекте информационная среда проекта может стать тормозом для выполнения проекта. Для разных типов проектов существует свой набор или пакет документов проекта. Например, документация проекта по строительству дома будет в себя включать: эскизный проект и технико-экономическое обоснование проекта строительства, рабочий проект, исходно-разрешительную документацию и др. В свою очередь, документация проекта по внедрению программного обеспечения должна содержать в себе описание автоматизируемых функций, описание постановки задач (комплекса задач), описание систем классификации и кодирования и др. ряд документов. **Перечень пакета документов по управлению Проектом :**

Устав проекта

- Описание содержания проекта
- Реестр заинтересованных сторон проекта

План управления проектом

Запрос на изменение в проекте

Лист согласования участия в проекте

Положение об управлении рисками

- План управления рисками
- Реестр рисков

Протокол совещания

Отчеты

- Отчет об исполнении работ по проекту
- Отчет о статусе проекта
- Отчет по завершению проекта

Ведение документации один из важнейших элементов любого проекта. Никто не любит писать документы... кроме тех, кто умеет. Используйте готовые шаблоны артефактов (текст, схемы, таблицы и презентации) и отчетных документов (deliverables). Но перед тем как начинать придумывать или заполнять готовые шаблоны, нужно ответить на три важных вопроса:

- Какие артефакты и документы нужны для вашего проекта?
- Насколько детально нужно их прорабатывать?
- Стоимость времени, потраченное на создание документа по отношению к ценности документа?

Генерировать кучу ненужных документов дорого, долго и глупо. Это выгодно, если проект оценивают по толщине отчетных документов. Но толстые документы никто не читает. Их ставят на самую дальнюю полку и забывают навсегда.

Поэтому нужно выбрать только те документы, которые нужны для достижения целей проекта. Для результатов. И прорабатывать их настолько детально, насколько это нужно для достижения целей проекта. Логично. Но как определить эту грань?

Рекомендую метод постепенного улучшения или по требованию, который представляет из себя следующую последовательность:

- Сначала выбирается минимальный набор документов.
- Заполняете на основании здравого смысла. Если что-то кажется лишним, отбрасывайте.
- Затем оцениваете, сможете ли вы с помощью этой информации достичь нужных результатов.
- Если нет, то включите недостающие разделы или документы.
- Заполните их и снова проведите оценку.
- И так далее до достижения результатов.

Инструменты по Управлению Проектами

Как и какие выбрать инструменты по управлению проектами. На рынке представлены десятки инструментов, от бесплатных до дорогих. Внедрение некоторых из них может стоить сотни тысяч долларов. Как и в случае выбора инструментов по управлению Архитектурой Предприятия, я рекомендую использовать по возможности бесплатные или дешевые инструменты.

Какие минимальные требования к инструментам? Что они должны помогать вам делать?

- Писать и редактировать тексты, составлять схемы, вести таблицы, делать презентации и т. д.
- Размещать их на общедоступном ресурсе, регулировать права доступа к информации, обсуждать эти материалы.

Набор инструментов :

- Для составления документов, схем, таблиц и презентаций можно использовать стандартный офисный пакет, например, MS Office. Для него есть готовые шаблоны для документов. Есть расширения для Visio, при помощи которых можно нарисовать все нужные схемы.
- Для совместной работы можно использовать корпоративный портал, систему управления документами, корпоративную почтовую систему, корпоративную систему передачи сообщений или выделенный файловый ресурс в корпоративной сети организации. Выбор решения будет зависеть от того, что уже есть у вашей компании.

Профессиональные инструменты по Управлению Проектами такие как:

- Microsoft Project 2016 Server / Professional
- JIRA Project Management

Для развитых организаций или проектных ИТ компаний желательно дополнительно использовать профессиональные системы, если они не входят в составе систем Управления Проектами, такие как:

- Система санкционирования выполнения работ (Work Authorization System).
- Система управления изменениями (Change Control System).
- Система управления конфигурацией (Configuration Management System).

Ключевые факторы успеха проекта

Шансы на успех внедрения проекта повышаются, если у проекта есть поддержка топ

менеджмента компании и объем работ уменьшен таким образом, чтобы минимально значимый для компании результат был достигнут в минимальные сроки и за минимальную стоимость. Кроме этого стоит уделять большое внимание планированию, рискам и получению обратной связи от заказчиков (внешних или внутренних).

Можно выделить следующие ключевые факторы успеха проекта:

Четкие цели. Для проекта жизненно необходимы четкие и понятные цели. Причем достижение этих целей должно быть важно для спонсора проекта и ключевых заинтересованных лиц.

Быстрые результаты. Проект должен обеспечивать достижение краткосрочных целей. Важно поддерживать интерес спонсора к проекту. Для этого нужно быстро достигать необходимых для компании результатов, которые он сможет записать себе в актив. Если ближайшие результаты будут через 3 года, то интерес к проекту сильно упадет.

Активно работать со всеми заинтересованными лицами. В рамках проекта часто решаются вопросы, которые требуют участия топ менеджмента, других важных и очень занятых людей. Найдите способы вовлекать их в проект. Конечно, не стоит их звать на все совещания или дергать каждый день по разным вопросам. Но вы можете привлечь в проект их доверенных лиц, присылать справку по проекту, для встреч с ними готовить списки вопросов с вариантами ответов.

Избегать революционных изменений. Они очень красиво выглядят на бумаге, но их тяжело реализовать в жизни. Метод постепенных улучшений часто более эффективен.

Отслеживайте ценность результатов. Для каждого архитектурного решения нужно оценить выгоды, сроки, затраты и риски. Их нужно обязательно согласовывать со спонсором и заинтересованными лицами. Результаты проекта должны давать ценность компании.

Обеспечить максимальное повторное использование ИТ активы организации. Все сломать и переделать – это долго и дорого. А ломать то, что действительно работает, глупо. Зачастую информационные системы и оборудование компании используются на 15—30% возможностей. Это отличная возможность для получения быстрых результатов с минимальными затратами.

Архитекторы и менеджеры проектов должны активно работать с бизнесом и ИТ проектами. А не генерировать гениальные идеи на основе «лучших практик». Работа «в поле» для многих начинающих архитекторов крайне некомфортна. Они боятся показаться некомпетентными. Хотя то, что ИТ специалисты знают глубже конкретные технологии, чем архитекторы, совершенно нормально. Как и то, что бизнес знает лучше, как работает компания. Работа с людьми – единственный способ достичь результатов.

Максимально использовать и распространять информацию. Основной актив архитектурного проекта – это информация. Нужно сделать доступ к ней максимально быстрым и удобным. А также рассказывать всем, что у вас есть и как они могут это использовать.

Контроль результатов реализации проектов. Для проектов реализации, которые часто делают внешние исполнители, важна формальная приемка результатов. Закрыв проекты актами и сбежал. Архитекторы должны собрать единую систему из результатов нескольких проектов. Поэтому держите руку на пульсе.

Говорить с людьми на понятном языке. Говорить с бизнесом на языке бизнеса. Говорить с ИТ на языке ИТ. Старайтесь избегать сленга и профессионального жаргона. Важность коммуникации часто недооценивают. Контролируйте не только, что вы говорите, но и как, когда и кому. Если вас не понимают, это ваша вина. И очень большая проблема.

Начинайте с пилотного проекта. На старте ваша основная цель – показать реальные результаты.

Определите «Шаг проекта» – это понятное вам элементарное конкретное действие. Как для каждого человека, так и для проекта, ширина шага может быть разная и зависит от различных факторов. Ширину «шага успешности» при управлении проектом можно определить с помощью пяти критериев:

- Достаточно знаний и умений для того, чтобы сделать шаг
- Шаг кратковременный по времени
- Шаг имеет низкий уровень риска
- Шаг поведенческий-конкретный
- Понятно, что будет успехом шага

Одна из самых частых ошибок при внедрении – это сидеть и ждать, пока к вам придут люди, чтобы обсудить проблемы. Не ждите – не придут. Идите сами к людям на всех уровнях, спросите про их проблемы. Расскажите, кому вы уже помогли, предложите помочь в решении их проблем и задач. Задавайте вопросы.

Помните о ценности. Каждое ваше предложение должно быть обосновано с точки зрения ценности для компании. Забудьте фразу: «Это будет более правильно с точки зрения архитектуры». Всегда помните про выгоды, сроки, затраты и риски. Не предлагайте революций без подробного экономического обоснования.

Не изобретайте велосипедов.

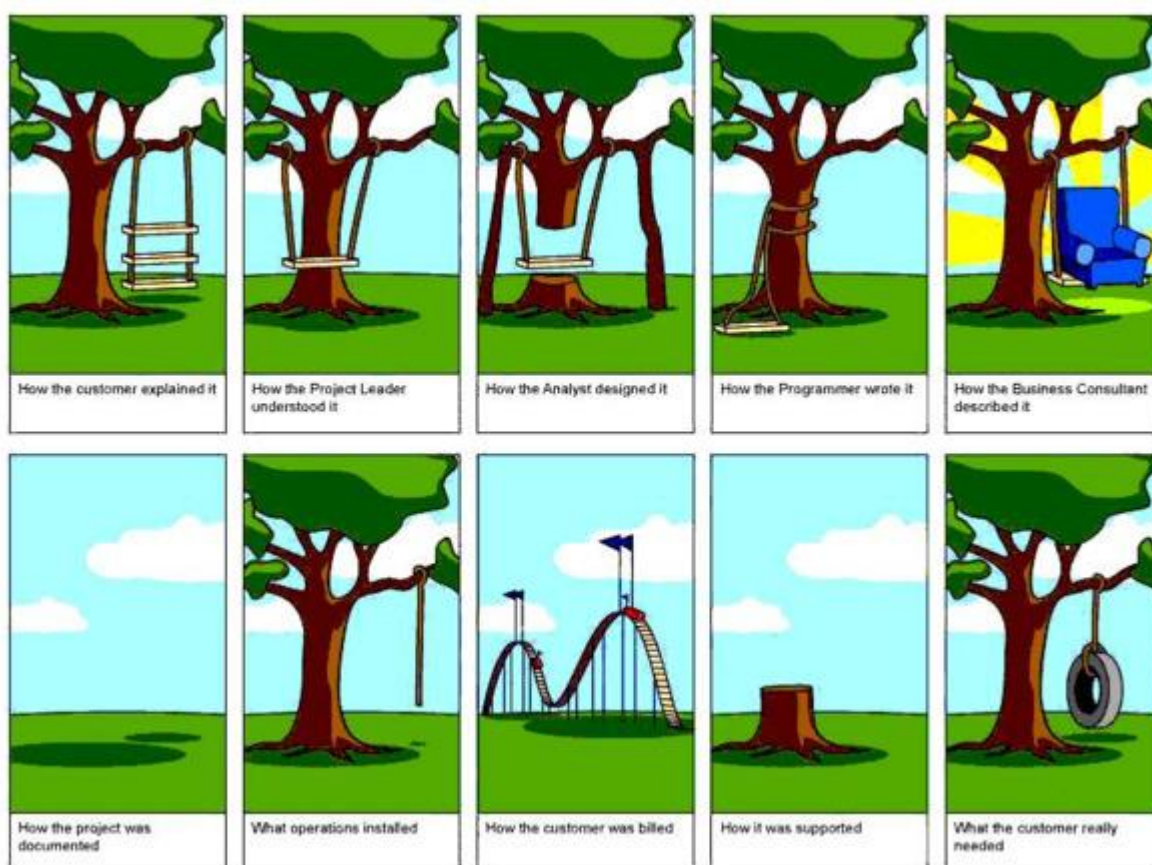
Не начинайте проект, не имея намерения его закончить . Два три вялотекущих или провальных проектов приведут к де-мотивации сотрудников.

Громко скажите «спасибо» руководству за поддержку, коллегам за помощь и терпение и т. д.

Основные причины провала проекта

Проекты, реализуемые без использования каких-либо методов, часто терпят крах по следующим десяти причинам:

- Проект представляет собой решение, приводящее к проблеме
- В конечном результате заинтересована только группа, работающая над проектом
- Никто ни за что не отвечает
- План проекта недостаточно структурирован
- План проекта недостаточно детализирован
- На реализацию проекта выделено недостаточно средств
- Выделенных ресурсов недостаточно для выполнения работ
- Проект не сверяется с планом его реализации
- Отсутствует взаимодействие между членами рабочей группы проекта
- Проект отклоняется от поставленной цели



При ведении любого проекта, в том числе и ИТ проекта, наиболее важными элементами являются процесс коммуникации всех вовлеченных подразделений и департаментов. Чем разнороднее участники (финансисты, представители бизнеса, ИТ и т.п.) тем важнее организовать коммуникацию на «одном» языке для всех участников проектной команды. В противном случае результаты проекта и его этапы могут быть похожи на диаграмму.

Заключение

Если подытожить результаты данной главы, то можно сделать следующие, на мой взгляд, важные выводы по методологии и техники управления проектами:

- *Классические методы* как «трактор» (если удачное завершение проекта, то как немецкий трактор) – «... сказали пахать – пашем с раннего утра и пока не вспашем...». Ориентирован на результат – выполнить любой ценной (как правило это конечный продукт, а стоимостью и временем как получится). Все делается по порядку и по инструкции.

- *Методология «PRINCE2»* – тоже самое, но задаются вопросом «... а на кой нам это нужно если дохода нет?...»

- «Вот „бабули“, больше нет – крутись как хочешь, но к завтрашнему утру чтобы было все готово. Что конкретно готово не знаем – но клиент сказал – ВСЕ». Это больше подходит на пример *использования гибких методов* управления проектами.

- «Пашем как молотилка» – *метод «SCRUM»*

- «KANBAN» присмотрит за тем, чтобы работники не были перегружены, а то «... сдохнут кони раньше времени...»

- *Методологии «LEAN» и «SIX SIGMA»* присмотрят за вопросом «... а не много ли косячат?...»

Ну а если серьезно, то важно отметить, что решения на все случаи жизни, даже

в рамках одной организации, не существует. Сфера управления проектами постоянно развивается, а знание менеджером проектов достоинств и недостатков каждой из методологий способствует успешной реализации проектов, расширяя потенциальные возможности всех заинтересованных сторон. Все методы управления проектами по-своему хороши и в каждом есть свои плюсы и минусы, применение методологии управления проектом очень сильно зависит от целей, типа и контекста проекта.

Концепция Управления Рисками

Общие Принципы

Управления рисками – процесс принятия и выполнения управленческих решений, которые направлены на снижение вероятности возникновения неблагоприятного результата и минимизируют влияние возможных потерь на организацию убытков, вызванных случайными событиями.

Данный раздел содержит основные принципы управления рисками при проектировании архитектуры, которые должны быть приняты во внимание. В процессе разработки и внедрения различных сервисов ИТ архитектуры необходимо проводить непрерывный процесс управления рисками. Для управления ИТ рисками можно воспользоваться как общими методиками так и специфичными для ИТ. Данная глава учитывает рекомендации стандарта «Управления и анализа рисков ISO 73: 2009», а также методика CRAMM v5 (CCTA Risk Analysis & Management Method) на основе требований организации CCTA (Central Computer and Telecommunications Agency) которая соответствует стандарту BS7799/ ISO17799.

Классификация рисков

Общую классификацию рисков можно представить, как:

Внутренние риски:

- Проектные,
- Технические,
- Технологические,
- Организационные,
- Финансовые и т п

Внешние риски:

- Природные,
- Политические,
- Социальные,
- Экономические и т п

По типу:

- Предсказуемые
- Не предсказуемые

По характеру:

- Преднамеренные
- Не преднамеренные

По виду:

- Прямые
- Косвенные

По результату:

- Нарушение функционирования,
- Нарушение целостности,
- Нарушение достоверности
- Нарушение конфиденциальности

По механизму воздействия:

- Аварии

- Ошибка персонала

Критерии оценки

К основным критериям оценки ценности ресурсов можно отнести следующие:

- Ущерб для репутации организации
- Безопасность персонала
- Разглашение персональных данных
- Разглашение конфиденциальных данных
- Разглашение коммерческой информации и сведений
- Санкции со стороны надзорных и государственных органов
- Финансовые потери
- Нарушения нормального функционирования организации

Основные шаги и стадии

В качестве основных шагов можно принять следующие действия:

Организация процесса управления рисками (General Risk Management)

- Разработка процесса, политик и процедур по Управлению Рисками
- Классификация ресурсов, рисков, уязвимостей, угроз
- Классификация реакции на риски и методов оценки
- Формирование комитета Управления Рисками
- Формирование экспертной группы, в состав которой входят специалисты ИТ, а также специалисты бизнеса.

Идентификация и оценка ресурсов (Identification and Valuation of Assets)

- Экспертная группа идентифицирует и оценивает ценность ресурсов
- Экспертная группа идентифицирует возможные риски

Оценка угроз и уязвимостей (Threat and Vulnerability Assessment)

- Экспертная группа оценивает уязвимости систем
- Экспертная группа оценивает угрозы систем

Анализ Рисков (Risk Analysis)

• Экспертная группа проводит качественный и количественный анализ рисков. В качестве основных критериев определяются: «вероятность» и «влияние» и классифицируются по значениям: «высокое», «среднее» и «низкое».

- Проводится количественный анализ рисков (при необходимости)
- Экспертная группа группирует риски и формирует матрицу (реестр) рисков

Основные механизмы и элементы анализа с технической стороны:

- *BIA (Business Impact Analysis)* – Анализ ИТ сервиса по уровню воздействия на бизнес
- *SFA (Service Fault Analysis)* – Анализ ИТ сервисов по уровню воздействия на связанные ИТ сервис
- *CFIA (Component Fault Impact Analysis)* – Анализ компонентов по уровню воздействия на ИТ сервис

Управление Рисками (Risk Management)

- Концентрируется внимание на рисках со значениями «высокое» и «среднее».
- Определяется реакция на риски (принятие, снижение, передача и т.п.)
- Определяются возможные контрмеры и стоимость их внедрения
- Формируется ряд сценариев проекта как минимум «негативный», «позитивный» и «реалистичный»
- Проведение корректировки
- Результаты документируются и принимается решение
- Все изменения в планах проекта должны обсуждаться и документироваться

Как минимум должны быть сформированы следующие документы:

- реестр рисков,
- запросы на изменение
- протоколы обсуждений.

В процессе эксплуатации ИТ сервиса проводится процесс управления рисками (поиск новых рисков, защитных мер и т.п.). Процесс является непрерывным и циклическим.

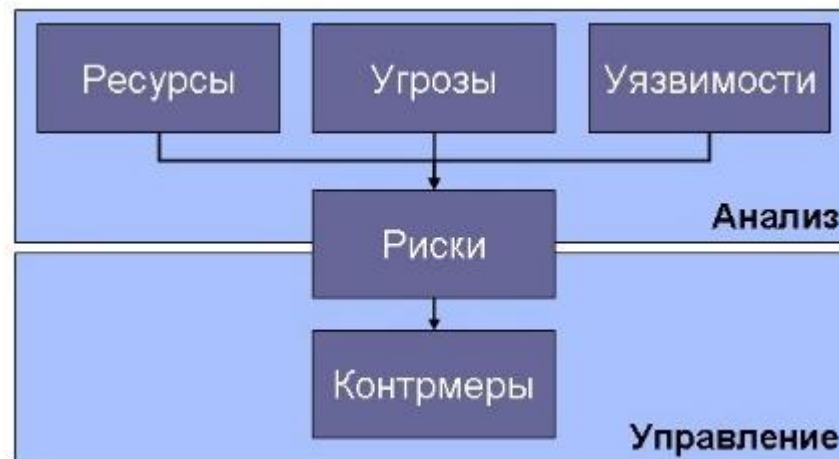


Диаграмма блок-схема анализа

Методы оценки рисков

В качестве методов оценки рисков можно использовать общеизвестные методы, такие как:

- Анкетирование
- Интервьюирование
- Комиссионный метод
- «Мозговой штурм» (Brainstorm)
- «Дельфи» метод (Delfy)

Наиболее распространённые инструменты, методики и техники оценки риска приводятся в международном стандарте ISO/IEC 31010:2009. В стандарте кратко описывается 31 метод оценки риска: мозговой штурм, анализ «Что если...», FMEA, HAZOP, НАССР, диаграмма «галстук-бабочка», анализ дерева отказов, Байесовы сети, FN-кривые и др.

Метод «Дельфи» или «Дельфийский метод» (Delfy Technique)

Метод сбора информации, используемый для достижения консенсуса экспертов по некоторому вопросу. В этом методе эксперты участвуют на условиях анонимности. Устроитель с помощью вопросника представляет идеи по важным моментам проекта, относящимся к данному вопросу. Ответы суммируются и возвращаются экспертам для комментариев. Консенсуса можно достичь за несколько циклов этого процесса. Метод Дельфи помогает преодолеть необъективность в данных и устраняет избыточное влияние отдельных лиц на исход обсуждения.

Суть метода «Дельфи» экспертных оценок заключается в том, что в результате серии действий независимых экспертов, формируется некоторое обобщенное мнение, являющееся более верное, чем мнение индивидуальных специалистов.

В процессе использования Дельфийского метода принимают участие две группы людей:

- Первая группа* – это эксперты, представляющие свою точку зрения на исследуемую проблему

- Вторая группа* – это аналитики, приводящие мнения экспертов к единому знаменателю

Сам же метод Дельфи подразумевает несколько этапов:

- Собирается группа

- Ставится задача
- Согласованность мнений

На первом этапе производится подбор экспертной группы. В неё может входить любое количество человек, однако рекомендуется формировать группу из 20 человек и не более.

На втором этапе выполняются следующие шаги:

Ставится проблема – эксперты получают основной вопрос, а их задачей является разбиение его на несколько более мелких. Аналитики производят отбор самых распространённых вопросов и составляют общий опросник.

Полученный опросник вновь представляется экспертам. Они должны сообщить, следует ли ещё что-то добавить, хватает ли данных, нет ли какой-то дополнительной информации по проблеме. Таким образом, получается 20 ответов (зависит от количества экспертов) с подробной информацией.

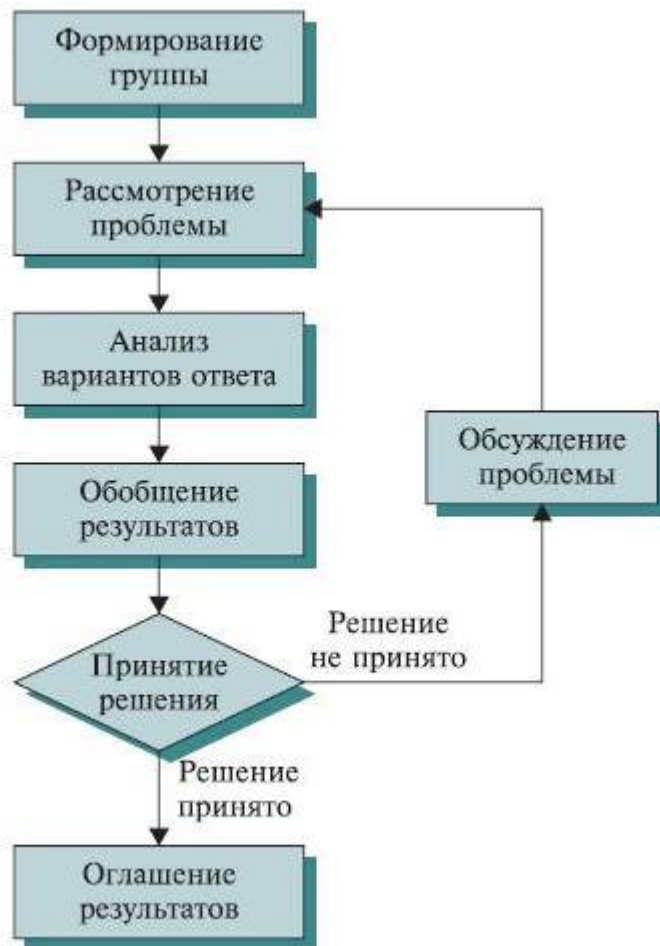
Аналитики составляют ещё один опросник. Новый опросник снова предоставляется экспертам. Теперь им нужно предложить свои способы решения проблемы и изучить альтернативные позиции остальных экспертов. Здесь производится оценка эффективности, наличия ресурсов, актуальности способов решения. Аналитики выделяют основные мнения экспертов и стараются их сблизить. Если чьи-то мнения идут в разрез с мнением большинства, эти мнения озвучиваются экспертам. В итоге, эксперты могут изменить свои позиции, после чего данный шаг снова повторяется.

Шаги повторяются снова и снова до тех пор, пока эксперты не придут к консенсусу, и не будет установлено единого мнения. А исследование аналитиками расхождений во мнениях членов экспертной группы может указать на незамеченные до этого тонкости проблемы. В конце концов, выносится общая оценка, и составляются практические рекомендации по решению проблемы.

И уже *на третьем этапе* проверяется согласованность мнений экспертов, анализируются полученные выводы и разрабатываются окончательные рекомендации.

Наряду с представленной структурой Дельфийского метода, существуют и другие модификации. Самая распространённая из них включает в себя бесструктурный этап. Используется данная модификация в том случае, если исследование направлено на поиск чего-либо конкретного, а организаторы исследования не способны сразу же представить проблему в форме специализированных вопросов. В этом случае уже на этапе формулировки проблемы привлекают экспертную группу.

Другая модификация метода Дельфи направлена на то, чтобы сократить время, которое будет затрачено на осуществление аналитического этапа – он называется «Экспресс-Дельфи». С учётом того, что традиционный метод со всеми его достоинствами является довольно трудозатраты и требует для своего применения значительного количества времени, экспресс-метод позволяет сохранить все основные элементы методики при том, что всю процедуру можно осуществить в течение нескольких часов, однако требуется специальная техническая база. Каждый член экспертной группы на протяжении отведённого временного периода находится за компьютером. Все компьютеры объединены одной общей сетью, которая замыкается на руководителе мероприятия. После того как эксперты предлагают свои решения в ускоренном режиме, аналитики точно так же должны как можно быстрее произвести оценки. Огромную роль в этом процессе играет оперативность в обработке и систематизации материала.



Достоинства метода:

- Метод Дельфи способствует выработке независимости мышления членов группы.
- Обеспечивает спокойное и объективное изучение проблем, которые требуют оценки.

Недостатки метода Дельфи:

- Организаторы мероприятия обладают чрезмерно большими полномочиями, по сравнению с экспертами, а значит, экспертов можно считать беззащитными в некотором смысле
- Коллективное мнение далеко не во всех случаях является верным
- Аналитики отбрасывают креативные решения, имеющие наименьшее количество сторонников, а эти решения могут быть самыми эффективными
- Невозможен оперативный анализ, т. к. для осуществления последнего этапа требуется много времени: каждый этап анализа может занимать минимум до 24 часов
- Эксперты склонны проявлять конформизм, испытывая желание и стремясь присоединиться к мнению большинства
- Организаторы имеют возможность манипулировать экспертной группой

Мозговой штурм (Brainstorming)

Мозговой штурм (Brainstorming) – Общий метод сбора информации, идей и предложения решений, который может использоваться для идентификации рисков, идей или решений проблем группой членов команды или экспертов. Обычно во время сессии мозгового штурма идеи участников фиксируются для последующего анализа. Это популярный метод группового взаимодействия, используемый для решения как образовательных, так и бизнес задач. Техника мозгового штурма направлена на спонтанное генерирование большого количества идей для решения какой-либо задачи или проблемы.

Этапы подготовки к проведению мозгового штурма:

- Постановка задачи
- Формирование группы участников
- Информирование участников обсуждения
- Составление списков мотивирующих вопросов

Постановка задачи/проблемы, которую необходимо решить. Проблема должна быть сформулирована кратко и, по существу. Если проблема слишком большая, то организатор должен разбить ее на краткие составляющие. Если же вопрос не может быть сформулирован кратко и не может быть разбит на составляющие, то мозговой штурм не является приемлемым методом решения такой проблемы.

Составление списка участников мозгового штурма. Наиболее продуктивна группа из 10 или чуть меньше человек. Кто должен входить в состав панели участников:

- Участники, уже посвященные в проблему или задачу.
- Участники, которые знакомы с родственной проблемой
- Один «собиратель идей», который фиксирует все предложенные идеи.

Составление и рассылка информационного письма участникам. Письмо должно содержать:

- название сессии,
- решаемую проблему,
- время, дату и место проведения.

Проблема должна быть описана в форме вопроса и нескольких прилагаемых к нему примеров идей.

Составление списка мотивирующих вопросов. Во время проведения обсуждений креативность может снизиться. Тогда организатору следует стимулировать активность мотивирующими к дальнейшей генерации идей вопросами.

Этапы проведения (работа с идеями):

•Перечисление идей без оценки реальности их воплощения. На этом этапе организатор представляет проблему, ставит простые вопросы в русле решаемой проблемы, а также обеспечивает безопасную среду для высказывания идей.

•Оценка идей с точки зрения их важности и вклада в решение проблемы. Каждая идея должна быть понята участниками. Для этого участники тщательно объясняют суть своих идей и их ценность для решения поставленной задачи.

•Категоризация собранных идей. На этом этапе похожие идеи формулируются в одну идею, а абсолютно нереальные/не важные идеи удаляются. Оставшиеся идеи должны быть четко сформулированы, поняты каждым участником и внесены в финальный список идей.

Основные правила:

•Фокус на количество: это означает, что должно быть выработано как можно большее количество разнообразных идей с прицелом на то, что чем больше их будет, тем больше вероятность найти среди них наилучшее решение. «Количество порождает качество».

•Сдерживание критики: любая критика должна быть сведена к «нулю». Вместо этого, участники должны быть сфокусированы на добавлении новых идей, оставив критику для следующей оценочной стадии.

•Разрешение необычным идеям: необычные идеи также должны быть внесены в список идей. Они порождаются взглядами с новых/других сторон и часто на их основе рождаются самые лучшие решения.

•Объединение и улучшение идей: лучшие идеи могут быть объединены в другую, еще более лучшую, идею (по типу «1+1=3»). Такое правило стимулирует создавать идеи посредством ассоциаций.

Стандартная методология M_o_R (Management of Risks)

Для оценки рисков и управления ими применяется стандартная методология M_o_R (Management of Risks), которая состоит из следующего:

Принципы M_o_R

Базируются на принципах управления организацией и являются необходимыми для эффективного управления рисками;

подход M_o_R – подход организации к указанным выше принципам должен быть отображен в ряде документов, в частности, в Политике управления рисками.

Процессы M_o_R

Выделяют четыре процесса в рамках M_o_R:

- Определение – определение угроз для деятельности, которые могут повлиять на достижение ею намеченного результата;
- Оценка – оценка суммарного влияния всех определенных угроз;
- Планирование – определение набора управленческих действий, которые уменьшат риски;
- Реализация – осуществление запланированных управленческих действий, их контроль, определение эффективности и корректирование в случае необходимости.

Пересмотр и внедрение M_o_R

Внедрение процессов, политик и подхода M_o_R так, чтобы они непрерывно контролировались и оставались эффективными;

Взаимодействие M_o_R

Обеспечение взаимодействия всех действий в рамках M_o_R с целью поддержки актуальности информации об угрозах, возможностях и других аспектах Управления рисками.

Кроме этого могут быть использованы специализированные методики:

Методика CRAMM v5

К специфическим ИТ методам и стандартам можно отнести методику CRAMM v5. Цель метода является создание формализованных процедур, позволяющих:

- Анализ требований, предъявляемых к Информационной системе, полон и документирован
- Идентификация и классификация рисков
- Идентификация и оценка уязвимости ИТ ресурсов
- Идентификация и оценка угроз ИТ системам
- Формирование обоснований для мер противодействия
- Избежать излишних расходов на обеспечение Информационной Безопасности систем
- Сокращение сроков по внедрению и сопровождению информационной безопасности организации
- Оказать помощь по вопросам функционирования ИТ сервисов на всех этапах жизненного цикла
- Автоматизация процессов анализа и управления рисками
- Оценка эффективности контрмер
- Формирование отчетов

Методология CORAS

Сочетание различных техник, таких как Event-Tree-Analysis, цепи Маркова и FMECA. В данном методе используется UML (Unified Modelling Language, язык программирования для визуального отображения объектов моделирования). Метод состоит из следующих действий:

- Поиск и систематизация данных об объекте анализа
- Определение объекта и субъекта, участвующие в анализе
- Полное описание процесса или задачи
- Проверка точности и полноты данных, представленных для анализа
- Осуществление действий по выделению рисков
- Оценка вероятности и последствий возникновения угрозы
- Ликвидация угрозы

Метод OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Метод быстрой оценки критических угроз, определения активов и выявления угроз. Характеризуется формированием специализированных групп и тесным вовлечением владельца бизнеса. Метод состоит из трех этапов:

- Оценка организационных аспектов

- *Комплексный анализ* информационной инфраструктуры организации
- *Разработка тактики* обеспечения безопасности и формирование стратегии. Состоит из следующих действий:

- ° Документирование текущего состояния
- ° Выбор подходов по сокращению рисков
- ° Выбор подходов по сокращению расходов
- ° Указывают изменения, необходимые для внесения в текущую организацию
- ° Выявляют перспективные направления работ по обеспечению информационной безопасности

Матричный Метод Анализа

Метод связывает активы, уязвимости и средства управления и определяет важность различных средств управления различным активам организации. Методология включает в себя три различных матрицы, связанные между собой:

- *Матрица угроз* – содержит в себе отношения между уязвимостями и угрозами.
- *Матрица уязвимостей* – содержит связь между активами и уязвимостями.
- *Матрица контролей* – содержит связи между угрозами и средствами управления.

Значение в каждой ячейке матрицы показывает ценность отношения между элементом строки и столбца. Используется следующая система оценок: 1 – низкая, 2 – средняя и 3 – высокая.

В процессе первоначального анализа формируются списки активов, уязвимостей, угроз и средств управления. Матрицы заполняются путем добавления данных о связи элемента столбца матрицы с элементом строки.

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие	Уязвимость										
	Активы и затраты	Торговые секреты	Конфиденциальная информация	Репутация	Потерянный доход	Затраты на восстановление	Информация	Аппаратные средства	Программное обеспечение	Обслуживание	Коммуникации
Веб-сервер											
Вычислительный сервер											
Брандмауэр											
Маршрутизатор											
Клиентские узлы											
Базы данных											

Затем данные из матрицы уязвимостей переносятся в матрицу угроз. Далее по такому же принципу данные из матрицы угроз заносятся в матрицу контроля.

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие	Угроза	Отказ в обслуживании	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных средств
Уязвимость							
Веб-сервер							
Вычислительный сервер							
Брандмауэр							
Маршрутизатор							
Клиентские узлы							
Базы данных							

Шкала 0 – нет воздействия 1 – слабое воздействие 3 – умеренное воздействие 9 – сильное воздействие	Угроза	Отказ в обслуживании	Вредоносный код	Ошибки пользователя	Внутренние атаки	Спам	Физическое повреждение аппаратных средств
Средства контроля							
Брандмауэр							
Система обнаружения вторжений							
Обучение персонала							
Политика безопасности							
Конфигурация архитек- туры сети							

Одно из преимуществ данной методики является ее универсальность

Определение	Формула	Переменные
Совокупное воздействие уязвимости V_i на активы организации вычисляется по формуле:	$V_i = \sum_{j=1}^n v_{ij} \times C_j$	п - Число активов a_j ($j=1, n$) - относительная стоимость актива V_i - уязвимость c_j - это воздействие уязвимости v_i на актив a_j. Р - Число угроз V_i - уязвимость d_{ki} - это потенциал воздействия угрозы t_k уязвимости v_i q - Число средств управления, которые могут смягчить р угрозу e_{ik} - воздействие средства контроля Z_0 на угрозу t_k.
Совокупное воздействие угрозы T_k определяется по формуле:	$T_k = \sum_{i=1}^m d_{ki} \times V_i$	
Совокупное воздействие средств контроля Z_0 определяется по формуле:	$Z_0 = \sum_{k=1}^p e_{ik} \times T_k$	

Формулы расчетов

Иерархическая структура рисков (Risk Breakdown Structure, RBS)

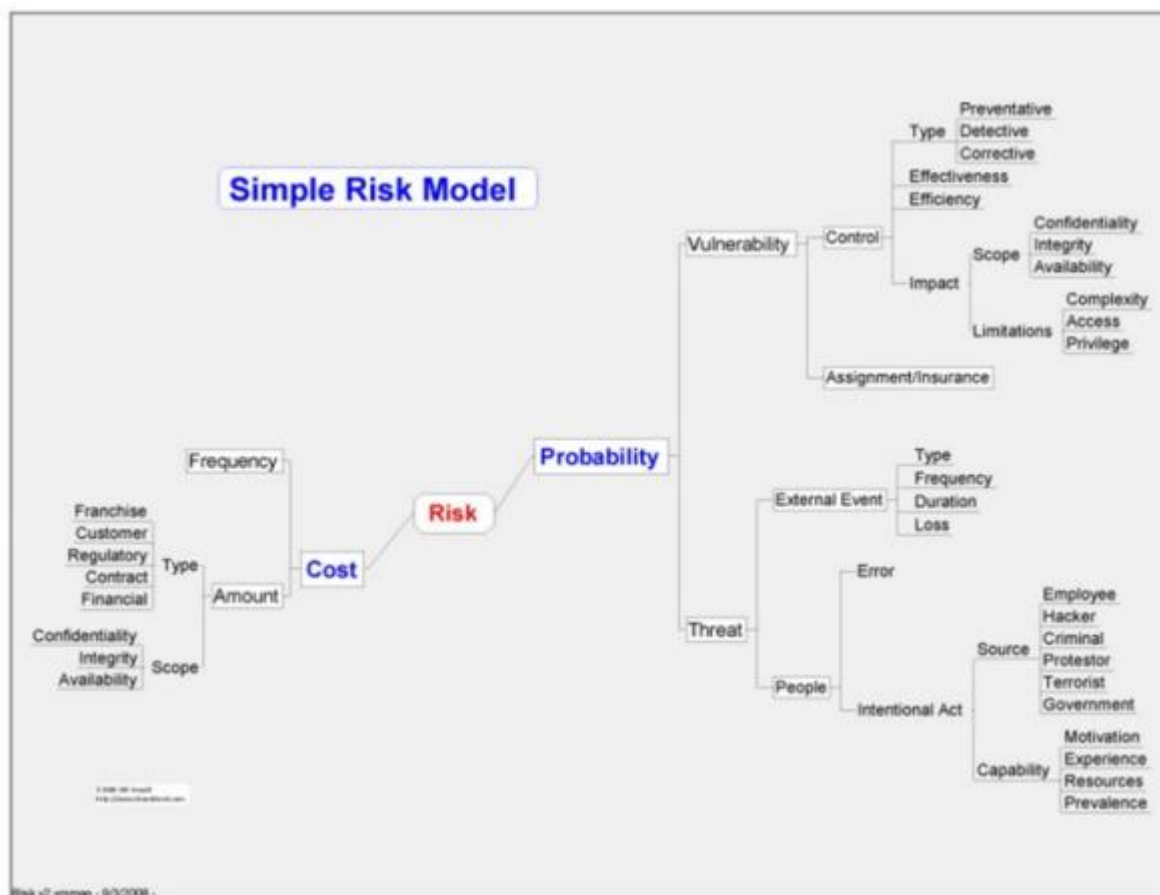
Иерархическая структура рисков (Risk Breakdown Structure, RBS) – Иерархически организованное представление известных рисков проекта, распределенных по категориям

и подкатегориям риска, указывающим различные области и причины возможных рисков. Иерархическая структура рисков часто подгоняется под конкретные типы проектов.

Методы расчета рисков

В качестве оценки рисков можно использовать как количественный, так и качественный метод оценки. Для количественного метода оценки рисков и угроз используются следующие показатели:

- SLE (*Single Loss Expectancy*) = Asset Value x EF (Exposure Factor)
- ALE (*Annualized Loss Expectancy*) = SLE x ARO (Annualized Rate of Occurrence)
- $Total Risk = Threats \times Vulnerabilities \times Asset Value$
- ACV (*Actual Cost Evaluation*)



Asset Value (AV) — Стоимость ресурса, отражает ценность ресурса. При качественном анализе можно использовать фиксированные величины (1 – низкая стоимость, 2- средняя и 3 – высокая стоимость). Например, сервер активного каталога будет иметь показатель $AV=3$, а рабочая станция $AV=1$.

Exposure Factor (EF) – Степень защищенности ресурса. Демонстрирует насколько данный ресурс подвержен угрозе. При качественном анализе можно использовать фиксированные величины (1 – низкая степень уязвимости или воздействия, 2- средняя степень уязвимости или большая вероятность восстановления ресурса и 3 – высокая степень уязвимости или возникнет необходимость замены ресурса). Например, сервер активного каталога будет иметь показатель $EF=2$.

Annualized Rate of Occurrence (ARO) – Оценка возможности возникновения угрозы. Указывает вероятность реализации конкретной угрозы за фиксированный промежуток времени (год). При качественном анализе можно использовать фиксированные величины (1 – низкая вероятность, 2- средняя и 3 – высокая вероятность). Например, сервер активного каталога будет иметь показатель $ARO=1$.

Annual Loss Exposure (ALE) – Оценка ожидаемых потерь вследствие воздействия определённой угрозы за определённый период времени. При качественном анализе можно использовать фиксированные величины (1 – низкая стоимость, 2- средняя и 3 – высокая стоимость). Например, сервер активного каталога будет иметь показатель AV=3, а рабочая станция AV=1.

При качественной оценке рисков можно воспользоваться следующей матрицей:

Оценка	Уровень последствий	Описание
0	Незначительные (Low)	Потеря конфиденциальности, доступности или целостности данных не ведет к финансовым, юридическим, репутационным или иным потерям
1	Умеренные (Moderate)	Потеря конфиденциальности, доступности или целостности данных ведет к незначительным или умеренным финансовым, юридическим, репутационным или иным потерям
2	Значительные (High)	Потеря конфиденциальности, доступности или целостности данных ведет к значительным финансовым, юридическим, репутационным или иным потерям, как по факту появления так и в последствии

Оценка последствий – оценка потерь, в результате появления факта риска.

Оценка	Вероятность появления	Описание
0	Малая (Low)	Вероятность появления риска при имеющихся механизмах контроля крайне низкая, появление новых инцидентов не ожидается
1	Умеренная (Moderate)	Вероятность появления риска при имеющихся механизмах контроля умеренная, появление новых инцидентов возможно но с малой вероятностью
2	Значительная (High)	Вероятность появления риска при имеющихся механизмах контроля высокая, появление новых инцидентов возможно но с большой долей вероятности

Оценка вероятности – оценка вероятности появления того или иного риска

№	Наименование	Описание	Владелец	Последствия	Вероятность	Уровень	Меры
1	Риск 1			0	2	2	Принятие риска
2	Риск 2			1	2	3	Разработка мер снижения риска

Таблица классификации рисков

Комбинация значений обеих таблиц (последствия + вероятность) ведет к определению уровня риска. Критерий уровня риска, который может быть принят (например, значения от 0 до 2) или непринят (например, значения от 3 и выше) определяется в соответствующем стандарте или политике в организации самостоятельно или в соответствии с требованиями или рекомендациями регуляторов. Основным критерий при ведении оценки рисков и разработки механизмов их снижения, стоимость контрмер не должна превышать стоимость средств защиты.

Реакция на риски

Влияние рисков может быть, как «негативное», так и «позитивное».

Для «позитивного» влияния риска может применяться следующая реакция:

- Использование (Exploit),
- Разделить (Share),
- Расширить (Enhance)
- Принять (Accept)

Для «негативного» влияния риска может применяться следующая реакция:

- Избегание (Avoid),
- Передача (Transfer),
- Снижение (Mitigate)
- Принятие (Accept)

Превентивные меры по реагированию на риски

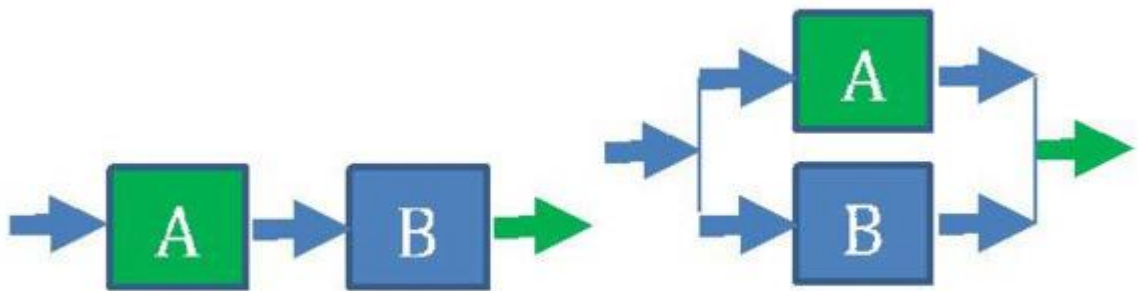
Для эффективного противодействия рискам и их последствиям рекомендуется учитывать следующую практику:

- Учет опыта аналогичных проектов
- Распределение рисков между участниками проекта
- Выделение ресурсов для управления проектами
- Планирование резервов
- Контроль за внесением изменений в план проекта
- Привлечение независимых экспертов
- Страхование рисков

Примеры расчета вероятности отказоустойчивости

Для примера возьмём устройства А и В (фаервол) с вероятностью безотказной работы 0.9.

Имеется два варианта включения устройств: «Последовательное» и «Параллельное» соответственно:



Последовательное и Параллельное включение

Рассчитаем *надежность первого решения*

Для «Последовательное» включения система откажет при поломке либо устройства А, либо В, либо обоих сразу.

$$P(AB) = P(A) * P(B) = 0.9 * 0.9 = 0.81$$

Надежность ниже, чем если бы работало одно устройство А или В.

Рассчитаем *надежность второго решения*

Для «Параллельного» включения система откажет только при поломке обоих устройств сразу.

$$P(A+B) = P(A) + P(B) - P(AB) = 0.9 + 0.9 - (0.9 * 0.9) = 1.8 - 0.81 = 0.99$$

Надежность выше, чем если бы работало одно устройство А или В.

На практике достаточно редко можно произвести точные расчеты по причине того, что отсутствуют достоверные входные данные. На мой взгляд, достаточно помнить простое правило:

•чем больше последовательно включенных элементов, тем ниже отказоустойчивость и доступность и выше сложность сопровождения

•чем больше параллельно включенных элементов, тем выше отказоустойчивость и доступность.

Концепция Управления Качеством

Общие Положения

Данный раздел содержит основные принципы управления качеством, которые должны быть приняты во внимание при проектировании архитектуры. При разработке концепции учитывались международные стандарты ISO 9000, ISO8402, BS7925—1.

Современная концепция управления качеством имеет в своей основе следующие основополагающие принципы:

- Качество – это неотъемлемый элемент любого проекта
- Качество – это то, что определяет потребитель, а не изготовитель
- Ответственность за качество должна носить адресный характер
- Повышение качества в современном мире зачастую зависит от уровня технологий
- Повышение качества возможно только усилиями всех сотрудников организации
- Контроль процессов более эффективен, чем контроль результатов
- Политика управления качеством должен быть общей политикой организации

Основные аспекты качества

- Качество обусловлено соответствием требований и ожиданий бизнеса, полноты и точности анализа
- Качество достигается за счет тщательной разработки проекта и его сопровождения
- Соответствие запланированных характеристик проекта или продукта его фактическим характеристикам
- Качеством материально-технического обеспечения на всем жизненном цикле продукта или сервиса

Основные процессы управления качеством

Quality Assurance (QA) – обеспечение качества. Это совокупность мероприятий, охватывающих все технологические этапы разработки, выпуска и эксплуатации ИТ сервиса, предпринимаемых на разных стадиях жизненного цикла, для обеспечения требуемого уровня качества.

Quality Control (QC) – контроль качества. Это совокупность действий, проводимых над продуктом или сервисом в процессе разработки, для получения информации о его актуальном состоянии в разрезе:

- готовность продукта к выпуску,
- соответствие зафиксированным требованиям
- соответствие заявленному уровню качества продукта.

Testing – тестирование. Одна из техник контроля качества, включающая в себя активности по планированию работ (Test Management), проектированию тестов (Test Design), выполнению тестирования (Test Execution) и анализу полученных результатов (Test Analysis). Условно можно разделить на две категории:

Верификация (Verification) – процесс оценки системы или её компонентов с целью определения удовлетворяют ли результаты текущего этапа разработки условиям, сформированным в начале проекта.

Валидация (Validation) – это определение соответствия, разрабатываемого ПО ожиданиям и бизнес требованиям.

Quality Improvement (QI) – повышение качества. Это совокупность мероприятий, для обеспечения улучшения или повышения уровня качества.

Участники процесса и их роли

Основные участники процесса контроля, управления и анализа качества являются рабочие и экспертные группы, в состав которых могут входить:

- Руководство бизнеса
- Департамент Внутреннего Аудита как владелец процесса управления качеством,
- Бизнес подразделения (в случае проектов, связанных с ИТ) портфелей, как заказчики ИТ сервисов
- ИТ департамент в составе экспертной группы ИТ специалистов, управление качеством ИТ сервисов
- Возможно участие сторонних консультантов

Концепция Управления Проектами и Контроля Качества «Шесть сигм» (six sigma)

Концепция «шесть сигм», которую иногда называют методологией, была разработана компанией Motorola для исключения лишних потерь, улучшения процессов и повышения прибыли. Основная цель SIX SIGMA – улучшение процессов и качества продукции за счет снижения дефектов или ошибок. Рейтинг/градация «6 сигма» означает, что 99,99966% от того, что производится – является бездефектным. Проверка процессы производства в целом, Вы можете найти возможные улучшения и доработки даже перед появлением дефектов. Методология, построенная на основе анализа данных, включает три ключевых компонента:

- DMAIC (define, measure, analyse, improve and control)* – определение, измерение, анализ, улучшение и контроль;
- DMADV (define, measure, analyse, design and verify)* – определение, измерение, анализ, проектирование и проверка;
- DFSS (Design for Six Sigma)* – проектирование для шести сигм. DFSS может включать как предыдущие, так и другие варианты: например, IDOV (identify, design, optimize and verify) – идентификация, проектирование, оптимизация и проверка.

Данная методика ориентирована на получение высокого уровня качества, единичных ошибки на миллион операций (стандартный метод «4 Sigma» порядка шести тысяч ошибок на миллион операций).

- Основные базовые принципы:
- Интерес к клиенту
- Управление на основе фактов
- Ориентированность на процесс, управление и улучшение
- Проективное управление
- Прозрачное взаимодействие (внутри организации без административных и иерархических барьеров)
- Стремление к совершенству и принятие неудач

Основы метода «6 Sigma» можно сформулировать цепочкой (замкнутым циклом) действий DMAIC

Определение (Define):

- Точное определение проблем и целей
- Выявление требований клиентов

Измерение (Measure):

- Сбор исходных данных
- Проведение измерений
- Статистическая оценка

Анализ (Analyse):

- Анализ данных и процесса
- Определение взаимосвязей
- Идентификация и верификация причин

Улучшение (Improve):

- Систематический поиск и выбор оптимального решения
- Реализация оптимального решения

Контроль (Control):

- Последовательное и долговременное определение уровня качества
- Управление процессом

Основные отличительные черты метода:

- Наличие сильного руководителя
- Результаты должны быть измеряемы
- Градация сотрудников по уровню компетенции
- Принятие решений только на основе проверенной информации, а не домыслов и предположений

В концепции 6 сигма уделяется отдельное внимание устранению возникающих проблем.

Конечная цель проекта – удовлетворение заказчика качеством продукта, которого можно добиться при помощи непрерывного процесса улучшения всех аспектов проекта, основанном на тщательном анализе показателей. При рассмотрении методологии с точки зрения управления проектами цепочка была предложена цепочка процессов из 5 шагов, известных как DMEDI:

Определение (Define): Первый этап очень похож на ранние этапы других систем проектного управления. На нём определяется содержание проекта, собирается информация о предпосылках проекта, ставятся цели.

Измерение (Measure): 6 сигм ориентирована на сбор и анализ количественных данных о проекте. На данном этапе происходит определение, какие показатели будут определять успех проекта и какие данные нужно собирать и анализировать.

Исследование (Explore): На стадии исследования менеджер проекта решает, каким же образом команда может достичь поставленных целей и исполнить все требования в срок и в рамках бюджета. На данном этапе очень важно нестандартное мышление руководителя проектов при решении возникших проблем.

Разработка (Develop): На данном этапе реализуются планы и решения, принятые на предыдущих этапах. Важно понимать, что на данном этапе необходим детальный план, в котором описаны все действия, необходимые для достижения поставленных целей. Также на данном этапе измеряется прогресс проекта.

Контроль (Control): Ключевой этап в методологии 6 сигм. Его основная задача – долгосрочное улучшение процессов реализации проектов. Данный этап требует тщательного документирования извлечённых уроков, анализа собранных данных и применения полученных знаний как в проектах, так во всей компании в целом.

Lean BB DMAIC	Define	Measure	Analyze	Improve	Control
Purpose	- Define Business Metrics - Identify projects for process improvement - Select resources for project improvement	- Establish baseline performance - Validate measurements for each project	- Set performance objectives - Identify sources of variation	- Prioritize the vital few causes of variation - Establish relationships between output and input variables	- Implement Solutions - Ensure Solutions are sustained - Document Case Studies
Primary Tools	1. Voice of the Customer 2. Business Metrics 3. Trend Charts 4. Process Mapping 5. Value Stream Map 6. Value Stream Measurements	1. Data Collection 2. Descriptive Statistics 3. Six Sigma Metrics 4. Measurement System Analysis 5. Basic SPC 6. Process Capability Analysis 7. Process Analysis 8. Process Cycle Time	1. Data Collection Forms 2. Control Charts 3. Hypothesis Testing 4. Cause & Effect Diagrams 5. Affinity Diagrams 6. FMEA 7. Root Cause Verification 8. ANOVA	1. Design of Experiments 2. FMEA 3. Planning Tools 4. Process Capability Analysis 5. Measurement Capability Analysis 6. TPM 7. 5S 8. SMED 9. Kaizen 10. Solution Selection Matrix	1. Mistake Proofing 2. SPC Implementation 3. Control Plans 4. Process Standards 5. Evaluate Process improvement results 6. Visual Management 7. Standard Operating Procedures 8. Dashboard
Key Outputs	- Project team - Project selection and measurement - Program plan - Management Commitment	- Product performance baseline - Measures for evaluating performance of the Product or Process	- Defined list of potential sources of variation - Cost Benefit Analysis	- Select appropriate solution - Proposed process settings - Impact of proposed solutions	- Process in Control - Project Documentation - Opportunities for transfer of learning

Методология «Шесть Сигм» более структурированная версия Lean нежели Kanban, в которую добавлено больше планирования для экономии ресурсов, повышения качества, а также снижения количества брака и проблем. «Шесть Сигм» очень похожа на Kanban, только с установленными этапами реализации задач – планированием, определением целей и тестированием качества. Вероятнее всего, встреч команды при применении «Шесть Сигм» будет значительно больше, чем при Kanban, но зато процесс реализации проектов более структурирован и команде сложнее сбиться с пути. Как и Kanban, «Шесть Сигм» можно относительно легко адаптировать к нуждам конкретной компании или команды. Жёстким требованием является лишь тщательное измерение и контроль показателей проекта на этапах реализации – без этого невозможно постоянное долгосрочное улучшение процессов реализации проекта. Описывается стандартами:

•«ISO 13053—1:2011 Количественные методы в процессах улучшения. Шесть сигм. Методология DMAIC»

•«ISO 13053—2:2011 Количественные методы в процессах улучшения. Шесть сигм. Инструменты и техники».

В последнее время, метод «6 Sigma» тесно переплетается с философией «LEAN» – бережливое производство.

Сильные стороны Концепция «Шесть Сигм» предоставляет чёткую схему для реализации проектов и постоянного улучшения процессов. Определяя цели, затем тщательно анализируя их и пересматривая вы получаете количественные данные для более глубокого понимания проекта и принятия более качественных решений. И хотя сбор, анализ данных и извлечение уроков могут занять определённое время, это позволит улучшить и оптимизировать процессы реализации проекта и сэкономить таким образом ресурсы в будущем. 6 сигм подходит для трудных проектов, в которых много новых и сложных операций. Данный подход позволяет реализовывать элементы проекта, учиться на ошибках и повышать качество в будущем.

Слабые стороны Проблема методологии «Шесть Сигм» в том, что, хотя основной декларируемой целью является снижение затрат и повышение эффективности, но удовлетворение заказчика часто вырывается на первый план. Учитывая некоторые различия в целях на разных этапах проекта, часто у команд возникает путаница в приоритетах, и избежать

этого не просто. Кроме того, основной лейтмотив «Шесть Сигм»: «Всё всегда можно сделать ещё лучше». Это может демотивировать сотрудников, не чувствующих удовлетворения от проделанной работы. Кроме того, если проект единичный и компания не планирует в будущем реализовывать подобные проекты, все затраты на анализ и извлечение уроков могут оказаться напрасными.

Управление Проектами и Концепция Бережливого Производства (LEAN)

LEAN (Бережливого производства/разработки) – концепция, инициатив по непрерывному улучшению процессов. Кроме выше упомянутого можно принять во внимание теорию ограничений «барабан – буфер – веревка». Суть методики в поиске и определении ограничений в процессе производства. При воздействии на ключевые элементы системы, можно добиться больших результатов, чем при одновременном воздействии на все компоненты. Суть элементов:

- Барабан – производство работает по некоторому «ритму»
- Буфер – перед ограничением должен иметься буфер (ресурсов) для предотвращения простоя производства
- Веревка – материалы должны подаваться только когда они достигли своего разрешенного минимума

Задачи LEAN или бережливое производство, заключается в создании ценностей высокого уровня и обеспечении высочайшего качества работы с меньшими трудовыми ресурсами, средствами и временем. Lean сокращает потери, устраняя узкие места, фокусируясь на ценностях потребителя и постоянно улучшая процесс производства. Использование Lean помогает сократить расходы, оперативно выполнять работу в поставленные сроки, достигать существенных результатов в составе малочисленных команд, привлекая к выполнению задачи минимальное количество человеческих ресурсов.

Объединяя эффективность системы Lean с шестью сигма, появляется возможность улучшить производственный процесс. Определив, как в действительности выполняется производственный процесс, члены команды проекта устраняют потери и сосредотачиваются на создании конечного результата с максимально высоким качеством для клиента (создание конечной ценности для потребителя).

Agile говорит нам, что необходимо разбивать на небольшие управляемые пакеты работ, но ничего не говорит о том, как управлять разработкой этого пакета. Scrum предлагает нам свои процессы и процедуры. Lean же, в свою очередь, добавляет к принципам AGILE схему потока операций (workflow) для того, чтобы каждая из итераций выполнялась одинаково качественно. В Lean, так же, как и в Scrum, работа разбивается на небольшие пакеты поставки, которые реализуются отдельно и независимо. Но в Lean для разработки каждого пакета поставки существует поток операций с этапами, подобными тем, которые были созданы для проекта Аполлон. Как и в классическом проектном менеджменте, это могут быть этапы планирования, разработки, производства, тестирования и поставки – или любые другие необходимые для качественной реализации проектов этапы.

Этапы Lean и их гибкость позволяют быть уверенными в том, что каждая часть проекта реализуется так, как требуется. В Lean не прописаны чёткие границы этапов, как в Scrum прописаны ограничения Спринтов. Кроме того, в отличие от классического проектного менеджмента, Lean позволяет параллельно выполнять несколько задач на разных этапах, что повышает гибкость и увеличивает скорость исполнения проектов. Как и Agile, Lean это скорее концепция, образ мышления, нежели нечто высеченное в камне. Используя идеи Lean Вы можете самостоятельно создать систему, удовлетворяющую вашим требованиям в управлении проектами.

Сильные стороны – Если Вам нравятся идеи Agile, но проект требует очень ровного качества и чёткого исполнения, Lean предоставляет набор инструментов для того, чтобы удовлетворить эти требования. Lean сочетает гибкость и структурированность, как Scrum, но в немного другом ключе.

Слабые стороны – Не каждая часть проекта требует одинаково детальной и дотошной проработки и внимания. Но Lean предполагает именно такой подход к каждой задаче и этапу. Это основной минус применения Lean для крупных и неоднородных проектов. А ещё, в отличие от Scrum, Lean не предлагает чёткого рабочего процесса для реализации «кусочков» проекта, что способствует растягиванию сроков проекта. Эта проблема может быть решена при помощи эффективного руководства и чётких коммуникаций – главное помнить об этом.

Основные методы контроля качества

Метод «7 Основных (японских) инструментов контроля качества»

Метод представляет из себя набор инструментов для сбора и анализа информации, Методы предоставляют возможность для последующего анализа дефектов и контроля качества. Состав инструментов включает в себя:

- Лист Сбора Данных
- Гистограммы
- Потоковые диаграммы
- Схема Исикавы «Рыбья Кость» (причинно-следственная связь)
- Диаграмма корреляции (рассеивания)
- Контрольная карта Шухарта

Рассмотрим набор инструментов и методов более подробно.

Лист сбора данных

Наиболее простое решения по сбору первичных данных. Может проводится как вручную, так и с применением средств автоматизации. Может представлять из себя список причин, жалоб, сгруппированных по общему признаку в отношении к продукту, дням недели и т п.

Гистограмма

Изменение какой-либо величины с учетом частоты ее распределения. Обычно графически представляется в графическом виде как столбцы с данными.

Потоковая диаграмма

Графическое отображение последовательности операций в рамках отдельного процесса, с указанием альтернативных путей развития событий в случае выполнения определённых условий.

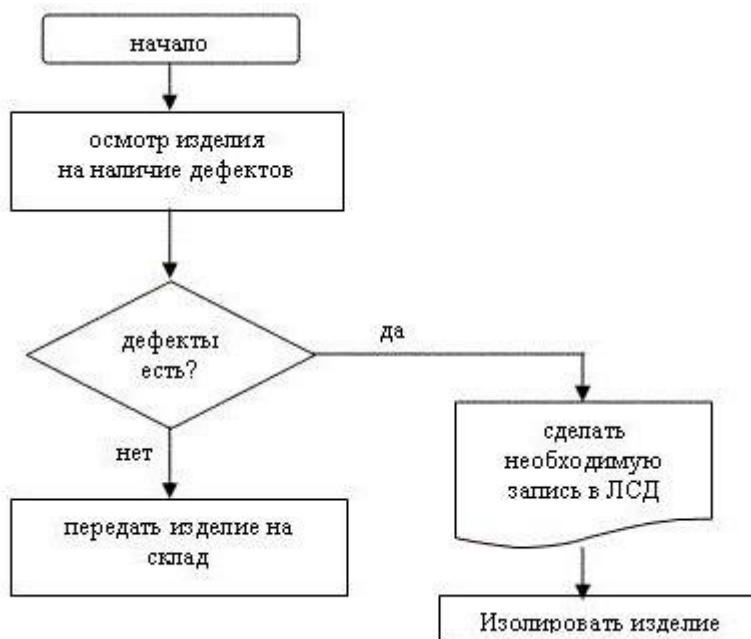
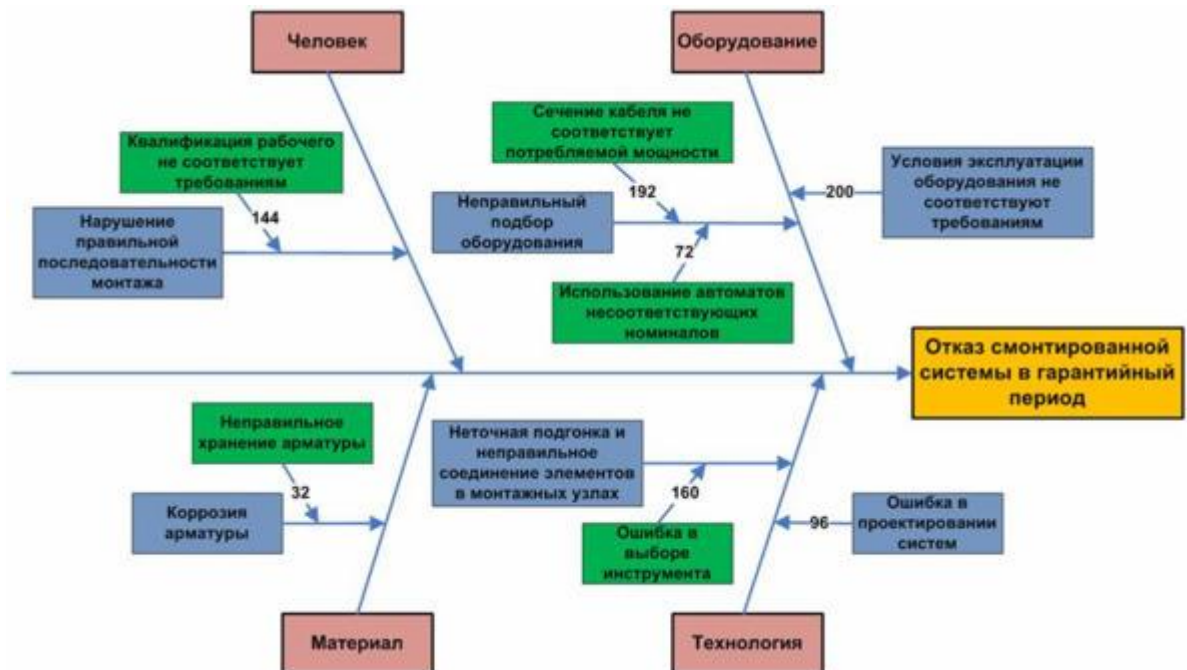


Схема Исикава «Рыбья кость» (причинно-следственная диаграмма)

Наиболее интересный инструмент, позволяющий формализовать и структурировать причины возникновения того или иного события, а также устанавливать причинно-следственные связи.



Все возможные причины классифицируются по пяти «5М» возможным категориям:

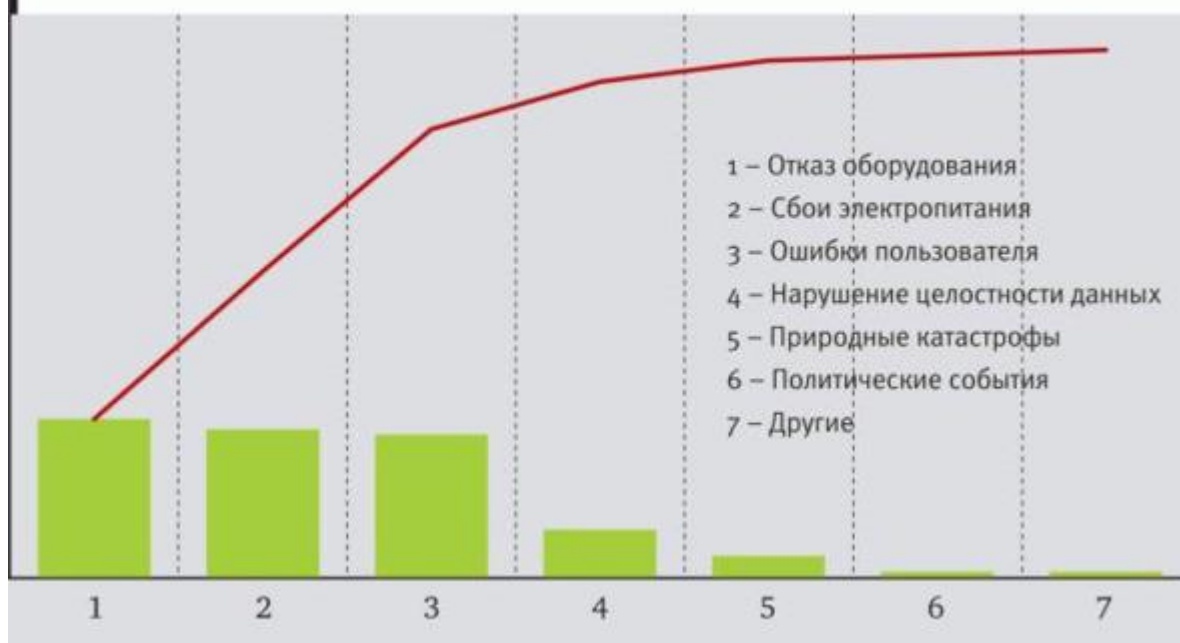
- Man – причины, связанные с человеческим фактором
- Machines – причины, связанные с машинами, техникой
- Materials – причины, связанные с материалами
- Methods – причины, связанные с методами, технологией и процессами
- Measurements – причины, связанные с методами измерений

К оси сходятся ветви «причины», каждая из которых состоит из «веточек», приводящих к возникновению причины. Все это ведет к результату «голове рыбы» – следствию.

Диаграмма Парето (Pareto Chart)

Принцип Парето гласит: *20% процентов причин порождает 80% процентов проблем.* Диаграмма помогает визуально выявить основные причины, оказывающие наибольшее влияние на возникновение той или иной проблемы.

Факторы, влияющие на надежность ИТ-систем



Данная диаграмма позволяет с помощью минимальных направленных действий эффективно решать проблемы. Следующие 30% процентов причин порождают порядка 15% процентов проблем. И наконец оставшиеся 50% процентов причин создают не более 5% проблем.

Обратный тезис «для устранения оставшихся 20% процентов проблем потребуется порядка 80% процентов ресурсов» также верен.

Диаграмма корреляции (рассеивания)

Визуальное отображение отношения между переменными величинами, связанными между собой. Как пример можно связать появление новых работников в организации и увеличение количества ИТ инцидентов.

Контрольная карта Шухарта

Наблюдение за протеканием процесса для выявления отклонений от нормального хода событий. Требуется наличие предварительной собранной информации. Горизонтальные линии отображают допустимые границы, контрольные карты могут различаться по двум основным признакам:

- *качественные показатели* (годен не годен, и т. п.). Существует четыре типа карты для данного признака:

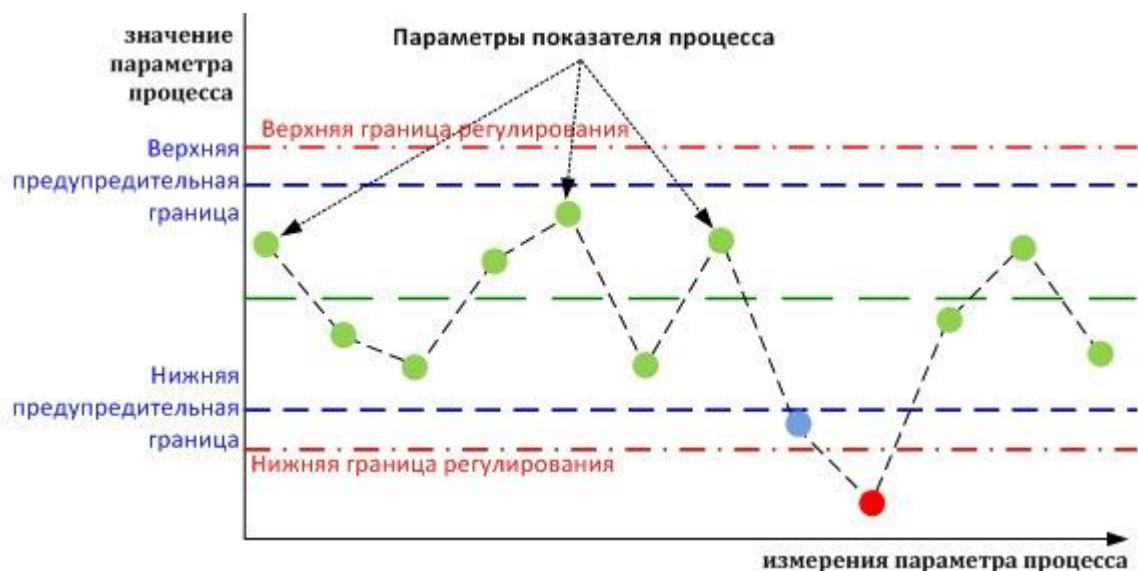
- U – карта (число дефектов на единицу продукции в переменном объеме выборки)

- C – карта (число дефектов в постоянном объеме выборки)

- P – карта (доля дефектных изделий в переменном объеме выборки)

- NP – карта (число дефектных изделий в постоянном объеме выборки)

- *количественные показатели*



Кроме этого существуют другие методы

Анализ характера и последствий отказов (Failure Mode and Effect Analysis, FMEA)

Анализ характера и последствий отказов (Failure Mode and Effect Analysis, FMEA) – анализ причин и последствий отказов. Метод анализа, применяемый в менеджменте качества для определения потенциальных дефектов (несоответствий) и причин их возникновения в изделии, процессе или услуге. Он применяется для выявления проблем до того, как они проявятся и окажут воздействие на потребителя.

Существует три основных вида FMEA, определяемых по объекту анализа:

FMEA – анализ технической системы. Направлен на выявление проблем в основных функциях системы;

FMEA – анализ конструкции. Направлен на выявление проблем в компонентах и подсистемах изделия;

FMEA – анализ процесса. Направлен на выявление проблем в процессах производства, сборки, монтажа и обслуживания изделия.

Они могут применяться каждый по отдельности, либо во взаимосвязи друг с другом. Если выполняются все три вида FMEA – анализа, то их взаимосвязь может быть представлена следующим образом:

FMEA – анализа связано с улучшением конструкции изделия (характеристик услуги) и процессов по его изготовлению и эксплуатации (предоставлению услуги). Анализ может применяться как по отношению к вновь создаваемым изделиям (услугам) и процессам, так и по отношению к уже существующим.

FMEA – анализ выполняется, когда разрабатывается новое изделие, процесс, услуга, или проводится их модернизация; когда находится новое применение для существующего изделия, процесса или услуги; когда разрабатывается план контроля нового или измененного процесса.

FMEA может проводиться с целью планового улучшения существующих процессов, изделия или услуги, или исследования возникающих несоответствий.

	Несоответствия	Последствия	Причины
FMEA – анализ системы	Несоответствия функций системы	Проблема	Причины проблемы
FMEA – анализ конструкции	Причины проблемы (из FMEA – анализа системы)	Проблемы для каждого элемента конструкции	Детальный список причин для каждого элемента конструкции
FMEA – анализ процесса	Детальный список причин (из FMEA – анализа конструкции)	Проблемы для каждого элемента конструкции (из FMEA – анализа конструкции)	Детальный список причин для операций процесса

FMEA – анализ выполняется в следующем порядке:

- Выбирается объект анализа. Если объектом анализа является часть составного объекта, то необходимо точно определить ее границы. Например, если проводится анализ части процесса, то для этой части необходимо установить начальное событие и завершающее событие.

- Определяются варианты применения анализа. FMEA может являться частью комплексного анализа, при котором применяются различные методы. В этом случае FMEA должен согласовываться с анализом системы в целом. Основные варианты могут включать:

- анализ сверху-вниз. В этом случае объект анализа разбивается на части и FMEA начинают проводить с наиболее крупных частей.

- анализ снизу-вверх. Анализ начинают с наиболее мелких элементов, последовательно переходя к элементам более высокого уровня.

- анализ компонентов. FMEA выполняют для физических элементов системы.

- анализ функций. В этом случае выполняют анализ функций и операций объекта. Рассмотрение функций осуществляется с точки зрения потребителя (удобство и безопасность выполнения), а не конструктора или изготовителя.

Определяются границы, в пределах которых необходимо рассматривать несоответствия. Границами могут являться – период времени, тип потребителя, география применения, определенные действия и т. п., например, несоответствия, выявляемые только при окончательном контроле и тестировании.

Разрабатывается подходящая таблица для регистрации информации. Она может изменяться в зависимости от учитываемых факторов. Наиболее часто применяется таблица следующего вида.

Определяются элементы, в которых возможно возникновение несоответствий (отказы). Элементы могут включать в себя различные компоненты, сборки, комбинации составных частей и пр. Если список элементов становится слишком большим и неуправляемым необходимо сократить границы FMEA.

В том случае если потенциальные отказы связаны с критическими характеристиками, дополнительно, при проведении FMEA, необходимо проводить анализ критичности отказов. Критические характеристики – это нормативы или показатели, которые отражают безопасность или соответствие нормативным требованиям и нуждаются в особом контроле.

Для каждого элемента, выделенного на шаге 5, составляется список наиболее значимых видов отказов. Эту операцию можно упростить, если применять стандартный список отказов для рассматриваемых элементов. Если проводится анализ критичности отказов, то необходимо определить вероятность появления отказа для каждого из элементов. Когда определены все возможные виды отказов для элемента, тогда суммарная вероятность их возникновения должна составлять 100%.

Для каждого вида отказа, выявленного на шаге 6, определяются все возможные последствия, которые могут проявиться. Эту операцию можно упростить, если применять стандартный список

последствий. Если проводится анализ критичности отказов, то необходимо определить вероятность возникновения каждого последствия. Когда определены все возможные последствия, вероятность их возникновения суммарно должна составлять 100% для каждого элемента.

Определяется рейтинг тяжести последствий для потребителя (S) – Severity. Рейтинг тяжести последствий обычно определяется по шкале от 1 до 10, где 1 означает незначительные последствия, а 10 катастрофические последствия. Если вид отказа имеет более одного последствия, то в FMEA таблицу вносится только наиболее тяжелое последствие для этого вида отказа.

Для каждого вида отказа определяются все потенциальные причины. Для этого может применяться причинно-следственная диаграмма Исикавы. Все потенциальные причины для каждого вида отказов заносятся в таблицу FMEA.

Для каждой причины определяется рейтинг вероятности ее возникновения (O) – Occurrence. Вероятность возникновения обычно оценивается по шкале от 1 до 10, где 1 означает крайне маловероятное событие, а 10 означает неизбежное событие. Значение рейтинга заносится в таблицу FMEA.

Для каждой причины определяются существующие методы контроля, которые применяются в данный момент, чтобы отказы не оказали влияния на потребителя. Эти методы должны предотвращать возникновение причин, снижать вероятность того, что произойдет отказ или обнаруживать отказ после проявления причины, но до того, как причина оказала влияние на потребителя.

Для каждого метода контроля определяется рейтинг обнаружения (D) – Detection. Рейтинг обнаружения обычно оценивается по шкале от 1 до 10, где 1 означает, что метод контроля абсолютно точно обнаружит проблему, а 10 – не сможет обнаружить проблему (или контроля вообще не существует). Рейтинг обнаружения заносится в таблицу FMEA.

Рассчитывается приоритетное число риска (риск потребителя – RPN) которое равно произведению $S * O * D$. Это число позволяет ранжировать потенциальные отказы по значимости.

Определяются рекомендуемые действия, которые могут включать изменение проекта или процесса для снижения тяжести последствий или вероятности возникновения отказов. Также могут предприниматься дополнительные меры контроля, чтобы увеличить вероятность обнаружения отказов.

После выполнения рекомендованных действий значения рейтингов S,O,D оцениваются заново, а приоритетное число риска RPN пересчитывается.

Анализ первопричины (Root Cause Analysis) и Анализ Дерева Отказов (Failure Tree Analysis FTA)

Аналитический метод, призванный найти основную причину отклонения, дефекта или риска. Одной первопричиной могут быть вызваны сразу несколько отклонений, дефектов или рисков.

Анализ дерева отказов – это методика идентификации и анализа факторов, которые могут способствовать наступлению некоторого нежелательного события (называемого вершинным («top events»)). Факторы-причины определяются дедуктивным способом, логически выстраиваются и представляются графически в виде диаграммы-дерева, которая изображает связь факторов-причин с основным событием. Достоинства метода:

- Графическое изображение того, как может возникнуть вершинное событие, с отображением взаимодействующих путей, когда два или более событий могут возникнуть одновременно;
- Список минимальных разрезов (отдельных путей к сбою) с вероятностями их возникновения (при наличии данных);
- Вероятность вершинного события

Концепция Управления Бизнес Процессами

Общие Положения

Данный раздел содержит основные принципы построения модели управления бизнес процессами, которые должны быть приняты во внимание при проектировании архитектуры. Для начала немного теории:

Термин BPM можно трактовать как:

- *Business Processes Modelling* (Моделирование Бизнес Процессов)
- *Business Performance Management* (Управление Эффективностью Бизнеса).

Бизнес процесс – совокупность мероприятий, направленных на создание продукта или услуги. Для наглядности обычно визуализируется в виде блоков. В контексте ИТ стратегии, может помочь ИТ департаменту понять бизнес деятельность организации и рекомендовать технологические инновации.

Реинжиниринг бизнес-процессов – это фундаментальное переосмысление и радикальное перепроектирование бизнес-процессов предприятий для достижения резких, скачкообразных улучшений в основных актуальных показателях их деятельности: стоимость, качество, услуги и темпы.

Реинжиниринг программного обеспечения – процесс создания новой функциональности или устранения ошибок, путём революционного изменения, но используя уже имеющееся в эксплуатации программное обеспечение.

Система по управлению бизнес-процессами (Business Process Management System – BPMS) – это структура для построения адаптируемых процессов. Система включает язык для моделирования бизнес-процессов (BPML), интерфейс дизайнера процесса, называемый системой счисления для моделирования бизнес-процессов (the business-process modelling notation – BPMN) и симулятор, который может быть использован для «летного» испытания нового дизайна процесса.

BPML – это открытая спецификация языка XML, и сегодня системы, использующие его, доступны. BPM не ускоряет разработку приложения, он просто устраняет необходимость в этом. BPM представляет собой важную инфраструктуру, основанную на существующих масштабируемых, отказоустойчивых системах по управлению данными и обработке транзакций.

Концепция управление бизнес процессами включает непрерывный анализ, оптимизацию, коммуникацию и внедрение бизнес-процессов в соответствии с требованиями рынка. Внутренние и внешние процессы компании – это ее нервная система. Она же является триггером для формирования ИТ стратегии, разработки, внедрения и сопровождения ИТ сервисов.

Процессный подход позволяет решить ряд вопросов, с которыми сталкивается организация в процессе своей бизнес деятельности:

- Оптимизация бизнес процессов
- Повышение производительности
- Снижение издержек
- Уменьшение времени
- Повышение качества
- Снижение операционных рисков
- Прозрачность, контролируемость и управляемость бизнесом
- Соответствие организационной структуры организации оптимальным бизнес процессам организации
- Проектирование новых и оптимизация имеющихся бизнес процессов
- Концентрация на основных бизнес процессах (создающих ценность) и оптимизация поддерживающих процессов
- Тиражирование и унификация бизнес деятельности
- Автоматизация деятельности
- Правильный и оптимальный подбор персонала
- Регламентация деятельности и высвобождение времени руководства
- Получение более точных финансовых показателей



Диаграмма управления бизнес процессами

Для грамотного построения бизнес-процессов, и Архитектуры Предприятия в частности, а также концентрации усилий и эффективного распределения ресурсов можно и нужно ввести классификацию бизнес-процессов. Подробная классификация бизнес-процессов имеет следующий вид:

Основными бизнес-процессами являются процессы, ориентированные на производство товара или оказание услуги, являющиеся целевыми объектами создания предприятия и обеспечивающие получение дохода. Так, для завода древесно-стружечных плит и деталей (ДСП и Д) основным бизнес-процессом является производство ламинированной древесно-стружечной плиты.

Сопутствующие процессы – процессы, ориентированные на производство товара или оказание услуги, являющиеся результатами сопутствующей основному производству производственной деятельности и также обеспечивающие получение дохода. Так, для автотранспортного предприятия процесс ремонта стороннего транспорта на собственной ремонтной базе является сопутствующим процессом.

Вспомогательные бизнес-процессы – процессы, предназначенные для обеспечения выполнения основных БП и поддержания их специфических черт. Так, для ТЭЦ или ГЭС вспомогательным бизнес-процессом является процесс ремонта производственного оборудования.

Обеспечивающие бизнес-процессы – процессы, предназначенные для жизнеобеспечения всех остальных БП и ориентированные на поддержку их универсальных черт. На предприятиях любой отрасли – это процесс финансового обеспечения деятельности, процесс кадрового обеспечения, инженерно-технического обеспечения и т. п.

Бизнес-процессы управления – это процессы, охватывающие весь комплекс функций управления на уровне каждого БП и бизнес-системы в целом. Это процессы стратегического, оперативного и текущего планирования, формирования и осуществления управленческих воздействий.

Бизнес-процессы развития – это процессы совершенствования производимого товара или услуги, технологий, модификации оборудования. Например, это проведение научно-исследовательских и опытно-конструкторских работ (НИОКР) в машиностроении, процесс технического перевооружения в электроэнергетике и т. п.

Методики и техники

Построение бизнес процессов возможно с использованием следующих методик:

- Аналитической дифференциации, разбиение общего процесса на его элементарные составляющие
- Синтетическая интеграция, обобщение родственных элементов процесса по функциональному, технологическому или прочему признаку.

Основные действия над процессами можно разделить на:

- Проектирование – создание новых процессов
- Перепроектирование – улучшение и корректировка имеющихся процессов
- Реинжиниринг – построение качественно новых процессов, на основе уже имеющихся.

Основные прикладные задачи при разработке бизнес процессов

Упорядочивание последовательности проведения операций:

- По принятию решения
- По исполнению решения
- По отражению принятых решений и результатов их исполнению

Создание методических рекомендаций и инструкций на каждой стадии:

- Документирование действий
- Формирование методических материалов
- Формирования материалов для сотрудников

Квалификационное разделение труда:

- Работа по управлению
- Работа основных специалистов
- Работа вспомогательных специалистов
- Создание ролей и формирование должностных инструкций

Видовое разделение труда:

- Обобщение однородных видов деятельности
- Концентрация специалистов на выполнение однородных действий
- Высвобождение высококвалифицированных специалистов от рутинной деятельности
- Автоматизация однородных действий

Изучение скрытых возможностей процесса

- Структурирование работы:
- Определение каждого элемента процесса
- Формирование алгоритма действий в рамках каждого элемента

Выявление и исправления проблем и дефектов.

Обмен информацией между подразделениями для понимания процесса с различных точек зрения.

Внесения ясности в понимание процессов за счет наглядности.

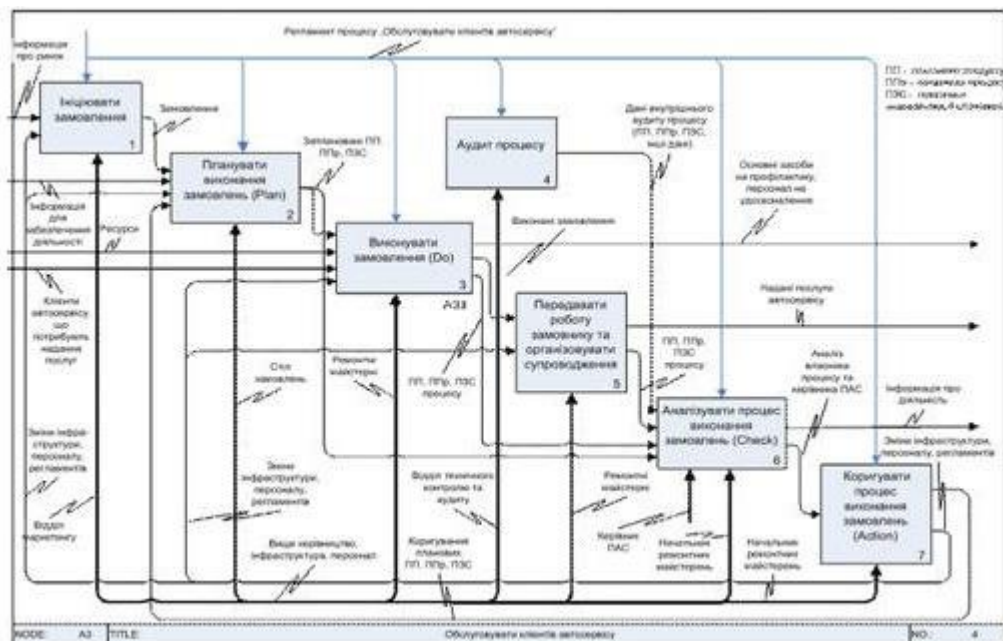
Для успешного внедрения процессного подхода можно использовать имеющиеся в мировой практике методики и инструменты:

- Business Process Model and Notation BPMN
- Диаграммный подход (Data Flow Diagram)
- IDEF0 и IDEF3
- Сетевой график PERT и диаграмма Gantt
- BAAN Diagram
- ARIS

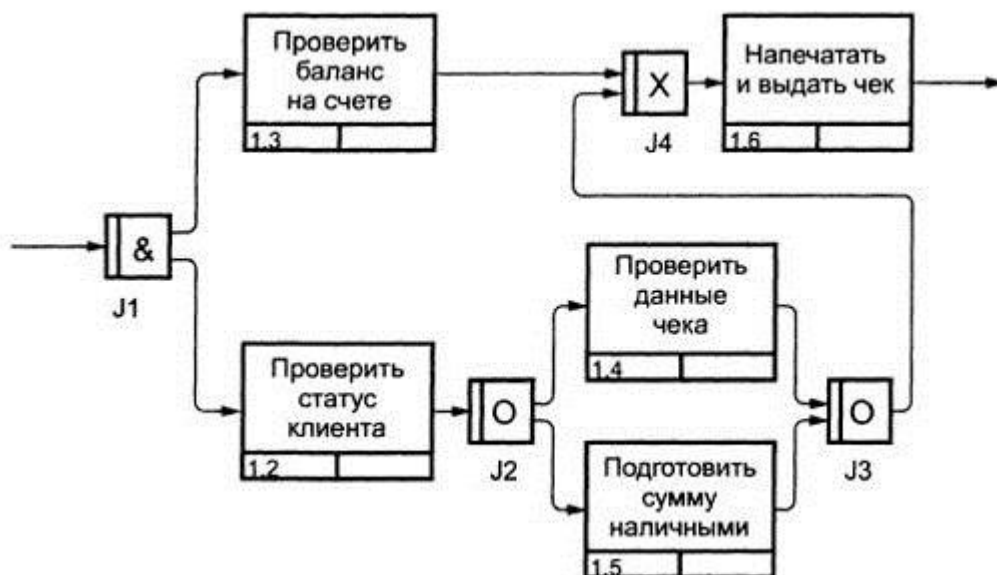
Методология IDEF (нотации IDEF0 и IDEF3)

Отличительной особенностью нотации является возможность декомпозиции, т. е. каждый отдельный блок в процессе в свою очередь может быть представлен в виде отдельного процесса.

Нотация IDEF0 обычно используется для описания процессов верхнего уровня, хотя и позволяет описать всю деятельность компании. Отличительной возможностью нотации является возможность отображения не только входов и выходов каждого блока, но и «управления» и «механизмов».



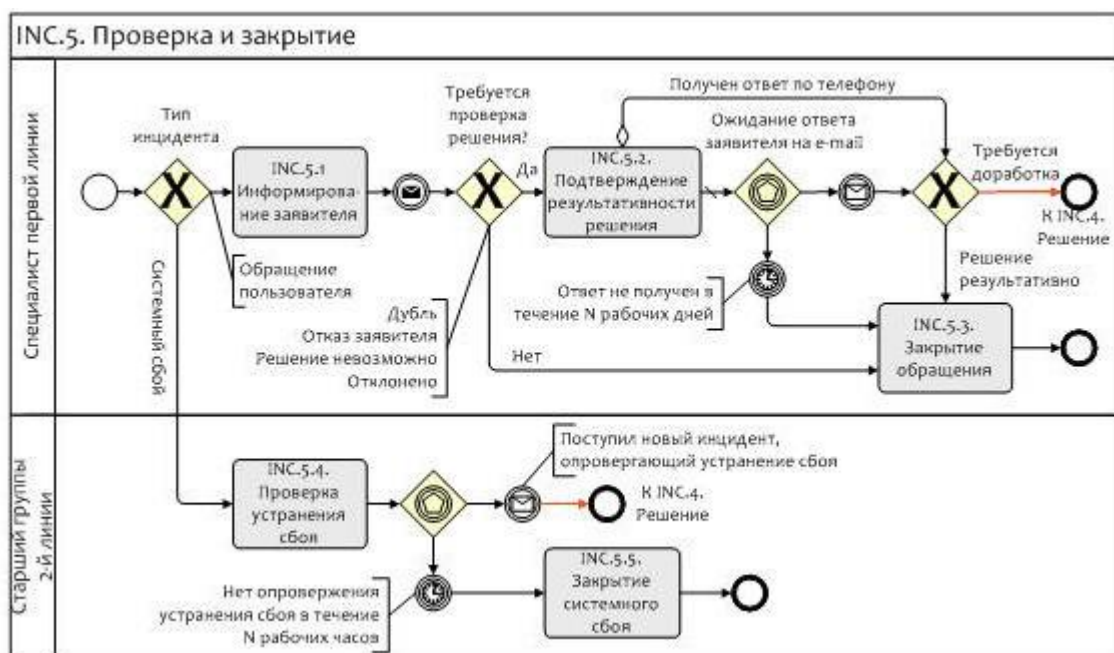
Обычно имеет ограничение на девять блоков. Вместе с дополнительными возможностями повышается и требования к квалификации бизнес-аналитиков, которые занимаются моделированием процессов в нотации IDEF0.



Нотация IDEF3 чаще применяется для построения процессов нижнего уровня, могут также использовать при декомпозиции блоков процесса IDEF0. В отличие от IDEF0 данная нотация не поддерживает отображение «механизмов» и «управления», зато отображает очередность выполнения работ персоналом.

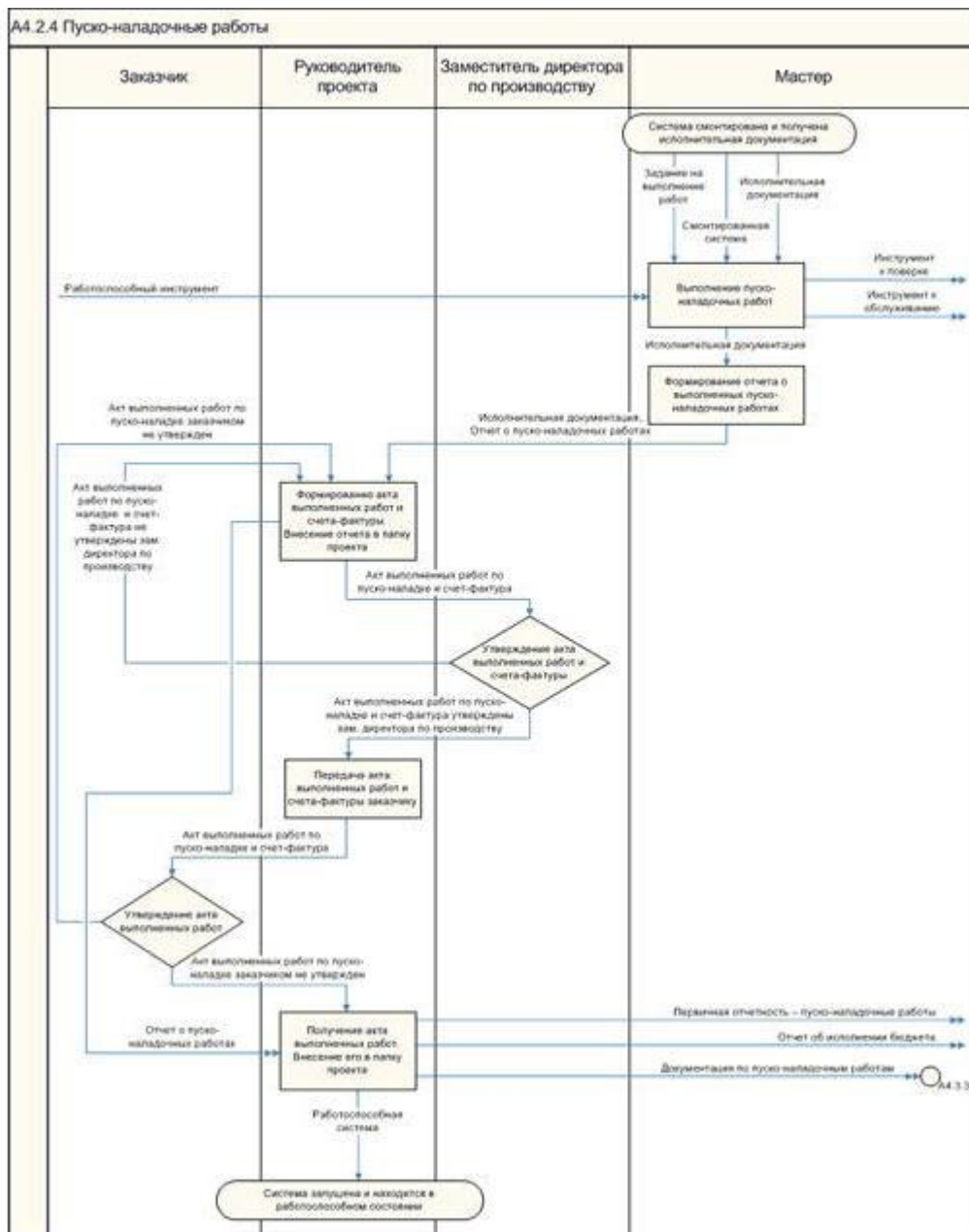
В нотации BPMN применяются логические операторы «И», «ИЛИ», а также их разновидности, как и в нотации IDEF3, но при этом существует возможность задание

циклических действий, выполняемых по определенному условию. В отличие от нотации серии IDEF, количество элементов на диаграмме неограниченно, а для лучшего визуального восприятия существует возможность сворачивать и разворачивать определенные части под-процесса.



Нотация BPMN обычно используется для построения диаграмм процессов нижнего уровня, описание процессов верхнего уровня для неё нетипично. Поскольку детальность описания процесса достаточно велика, существуют программные решения, которые способны преобразовать диаграммы в исполняемые процессы, эти процессы затем могут быть запущены сервером управления бизнес-процессами и обрабатываться в реальном масштабе времени.

Нотация Flowchart, известная также как «блок-схема», наверное, самый простой способ графического представления выполнения любого процесса. Блок-схемы часто применяются в учебных целях для отображения алгоритма выполнения какой-либо задачи. Для построения бизнес-процессов, в схему, как правило, вводят несколько дополнительных элементов: ответственность и ресурсы.



Нотация Flowchart наилучшим образом подходит для описания нижнего уровня процессов, но не предназначена для отображения взаимодействий на более высоких уровнях управления, поэтому многие разработчики программных продуктов применяют данную нотацию совместно с IDEF0 или разрабатывают собственную вариацию для построения процессов верхнего уровня.

Можно использовать аналог нотации Basic Flowchart с отображением ответственных за выполнение функции слева, а документов, регламентирующих её выполнение справа от функции, разделив функции на 4 типа и введя такие атрибуты как время и стоимость выполнения функции.

Процессы, построенные в нотации Flowchart наиболее наглядны и понятны даже неподготовленным сотрудникам компании.

В качестве инструментов построения бизнес процессов, можно воспользоваться: ARIS, ELMA, Business Studio, Visio, Fox Manager и т.п.

Дальнейшее развитие организации может потребовать применение специализированных решений (BPMS), которые позволяют не только моделировать процессы компании, но и внедрять их в рабочую среду и проводить мониторинг исполнения процессов. Помимо этого, ряд современных ERP решений уровня предприятия, имеют в своем составе функционал по моделированию процессов и непосредственного исполнения.

Алгоритм построения Бизнес Процессов

Для большинства организаций управление бизнес процессами можно представить в виде следующих этапов:

- Описание структуры организации «как есть»
- Анализ модели организации «как есть»
- Разработка структуры организации «как надо»
- Разработка плана перехода от модели «как есть» к модели «как надо»
- Внедрение необходимых изменений и измерений для достижения уровня «как надо»

Как одни из базовых циклов управления процессами можно выделить «Цикл Деминга»:

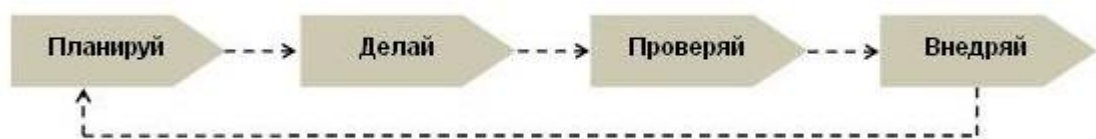


Диаграмма Цикл «Деминга Plan-Do-Check-Act PDCA»

Данный цикл является базовым для непрерывного процесса улучшения. Его более расширенный аналог, можно представить в виде цикла «Исикавы»:



Диаграмма Цикл «Исикавы»

Типичный бизнес-процесс включает в себя следующие компоненты:

•*Владелец процесса* – должностное лицо, имеющее права, полномочия и зону ответственности, а также распоряжающееся ресурсами процесса. Владелец процесса совсем не обязательно руководитель подразделения или предприятия. Это может быть просто специалист в той области, знание которой важно для качественного результата данного процесса.

•*Технология процесса* – порядок выполнения действий для преобразования входов в выходы. Система показателей (метрик) процесса – показатели качества продукта, эффективности процесса, удовлетворенности потребителей.

•*Управление процессом* – деятельность владельца процесса по его анализу и принятию управленческих решений.

•*Ресурсы процесса* – материальные средства, которые владелец процесса распределяет в ходе работ по процессу.

Описание бизнес процессов можно разбить на следующие шаги:

- Описание бизнес направлений
- Описание функций в бизнес направлениях. Может состоять из «горизонтальной» и «вертикальной» составляющих.
- Описание отделов и их продукты.
- Распределение функции «как есть»
- Распределение функций «как надо»

Бизнес процессы могут разбиты на под процессы. Цель получения минимальных под-процессов идентичной функциональности. Основные критерии:

- Определены границы процесса
- Работы ясны и понятны – элементарные однородные действия (функции)
- Имеется понятие конечного результата и метод его достижения
- Действия могут быть измеряемы и управляемы
- Возможно четко определить роли сотрудников

Для построения правильных бизнес процессов, рекомендуется производить декомпозицию по нескольким параметрам и получения нескольких «деревьев» процессов (например, по продуктам и сервисам, типам операций: покупка, продажа и т.п.) Кроме этого могут использоваться «Эталонные» (рекомендуемые) модели – схемы организации деятельности организаций, разработанные для конкретных отраслей и видов деятельности на основе реального опыта внедрения в различных компаниях по всему миру и включающие проверенные на практике процедуры и методы организации управления.

Цели организации обычно устанавливают, исходя из ее предназначения (миссии) и опираясь на принципы, которые культивирует руководство организации. При этом миссия в совокупности с принципами формирует политику, на основе которой и определяются цели. Политика организации (как и миссия, и принципы) определяется высшим руководством организации. Если цели и задачи установлены, но не определены способы их достижения и решения, управление останется голой теорией. Способы достижения целей и решения задач должны быть полезны для организации и не препятствовать ее развитию.

Ключ к успеху – решительная стандартизация очевидных вещей и передача их подчиненным.

Обучение и подготовка кадров способствуют формированию надежных работников, при этом, как правило, увеличивается норма управляемости (количество непосредственных подчиненных у одного руководителя). Можно организовать выполнение работ только лишь с помощью распоряжений, но такой процесс никогда не будет протекать гладко. Только опыт и квалификация работников помогают компенсировать несовершенства стандартов и регламентов.

Алгоритм построения бизнес процесса на примере процесса «Управления Инцидентами» в упрощенной схеме можно представить в следующей последовательности действий:

- Определение границ процесса
- Основные блоки процесса

- Детализирование блоков, разбивка на под-процессы
- Определение участников процесса и их роли
- Размещение документов, инструментов и действий над ними
- Определить метрики эффективности и механизмы измерений
- Связать схему с другими процессами и схемами (если таковые имеются)
- Проверить полученный бизнес процесс «тест на столе», с привлечением сотрудников ИТ и пользователей
- Утвердить процесс со стороны владельца бизнеса и передать на внедрение

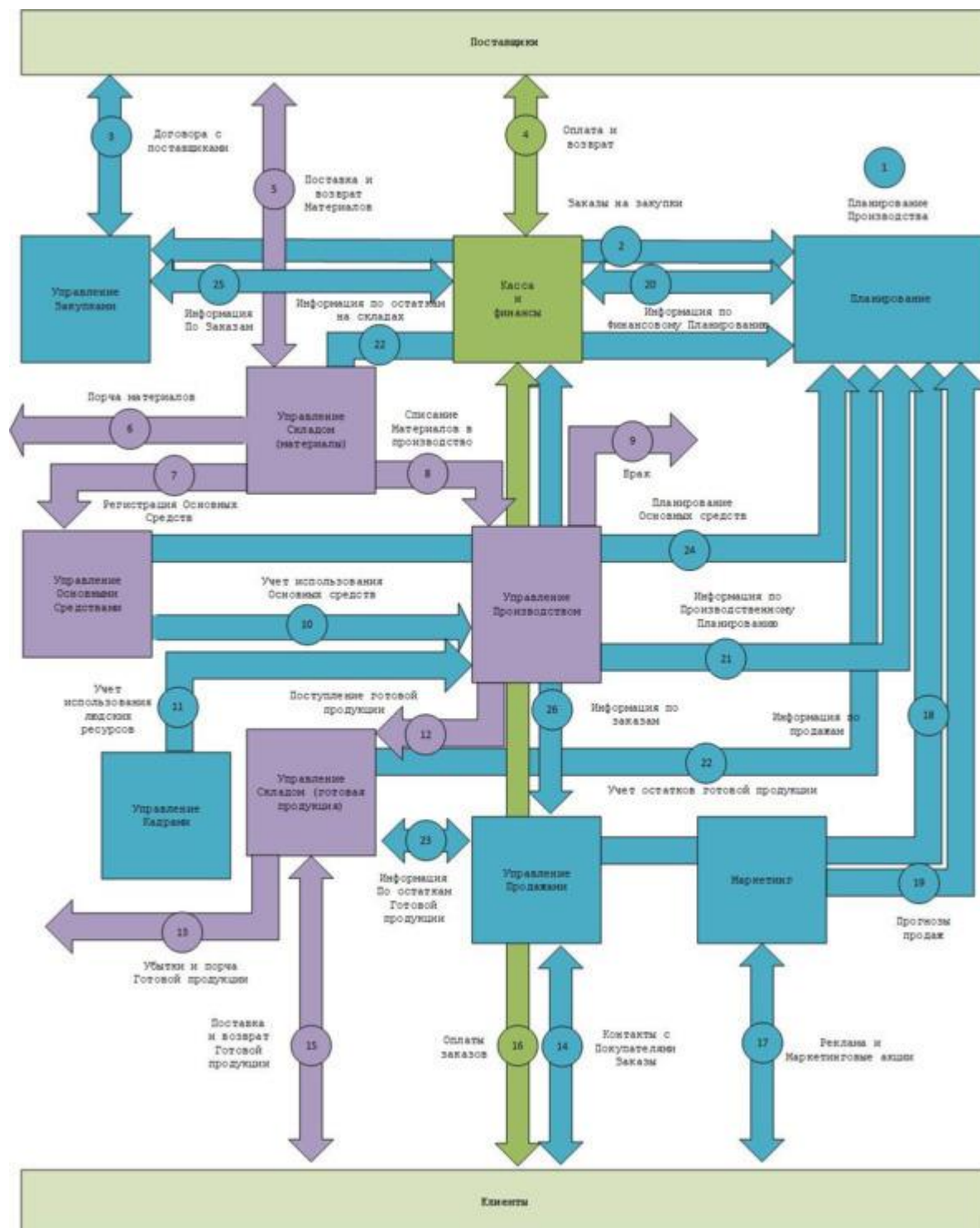


Диаграмма потоков ценностей в организации

Модели Деловой Активности (Patters of Business Activities PBA)

Модели Деловой Активности позволяют ИТ департаменту предоставить картину деятельности организации, что позволяет оценить требования к сервису, спроектировать, внедрить и сопровождать на уровне, удовлетворяющий требованиям бизнеса. Модели Деловой Активности фокусирует свое внимание на следующих параметрах, таких как:

- Частота (Frequency) – Как часто используется сервис
- Объемы (Volume) – объем активных действий, связанных с сервисом
- Продолжительность (Duration) – продолжительность активных действий, связанных с сервисом
- Место (Location) – определяет локацию (географическая точка, департамент и т п), где происходит активность,

Модели Деловой Активности также включают в себя профили пользователей (User Profile), который представляет из себя модель поведения пользователей сервиса.

Кроме выше сказанного, в модели деловой активности следует включать:

•уровень вовлеченности ИТ инфраструктуры в бизнес. Так, например, для банка, уровень вовлеченности ИТ в бизнес процесс высокий, потому что практически все бизнес процессы банка связаны с работой автоматизированной банковской программы и вовлечены порядка 70% сотрудников.

•возможности «обходных» решений при полном отказе ИТ сервисов. Обзор возможности ведения бизнеса при частичном или полном отказе ИТ инфраструктуры на определённые промежутки времени (час, день и т п).

Все это позволяет уже на начальном этапе стратегического планирования и разработки решений определить критичность тех или иных сервисов. Ниже приведены краткое описание различных моделей деловой активности различных отраслей бизнеса организации. Как пример можно рассмотреть деятельность банка.

Модель деловой активности Банка

Модель деловой активности Банка можно описать следующим образом:

- Деятельность банка тесно связана с функционированием ИТ инфраструктуры.
- Большая часть сотрудников банка работает с различными компьютерными системами (Автоматизированной Банковской Программой, системами переводов и т п).
- Компьютерные системы банка часто централизованы.
- Деятельность банка жестко регламентируется со стороны контролирующих органов.
- Высокие требования по вопросам физической безопасности.
- Высокие требования по вопросам информационной безопасности.
- Высокие требования к системам обеспечения ИТ инфраструктуры.
- Высокие требования по вопросам непрерывности предоставления ИТ сервисов.
- Время работы банка регламентируется, обычно пятидневная рабочая неделя, с 09:00 до 18:00. Оставшееся время может использоваться для проведения регламентных ИТ работ (создание резервных копий, архивирования, восстановления, проведение профилактических работ и т п)
- Наличие филиальной сети банка, географически распределенной по территории страны.
- Наличие сети банкоматов банка и POS терминалов.

Можно выделить основные бизнес приложения банка:

•Автоматизированная Банковская Программа (Automated Banking System ABS, Core Banking System SBS) – предназначена для ведения основной операционной деятельности организации. Характеризуется наличием механизма «закрытия дня» (Close of Business CoB) – фиксированием состояния операций. Система может иметь в своем функционале различные дополнительные возможности.

•Бухгалтерская программа (Accounting System AS) – система ведения бухгалтерского и налогового учета, и т.п. Как правило, операции бухгалтерии отстают по времени от основной операционной деятельности банка. Разделение ABS и AS систем требует настройка «однаправленной» интеграции данных.

•Специализированные платежные системы (такие как SWIFT, SWIFT/AZIPS, HONKS, APUS и т.п.) или терминалы платежных систем (Western Union, Contact и т.п.)

•Системы Интернет банкинга и системы онлайн оплат.

•Системы управления клиентами (CRM)

•Системы управления организацией (ERP)

•Наличие веб сайта

Профили пользователей и активности могут представлять из себя:

•Разделение по группам с фиксированными правами и доступами

•Жесткие ограничения на использование почты, интернета и систем конечных пользователей

Заключение

Суммируем все выше сказанное. С первой страницы главы и после первого определения BPM становится понятно, что ничего не понятно. Терминология и ее значение трактуется по-разному как в течении времени существования самого подхода, так и производителями «чудо» решения. В дополнение к основному термину, время от времени вводятся новые модные словечки: BPA (Business Process Automation или Business Process Analysis), BAM (Business Activity Monitoring), реинкарнация BPM (но уже как Business Process Monitoring) или же BPPM (Business Process Performance Management). Объединение гляцевых, «блестящих» словечек: Business Process Reengineering (BPR), Corporate Performance Management (CPM), Enterprise Performance Management (EPM), Strategic Enterprise Management (SEM) и прочие великое множество. Более детально об этом можно прочесть у Ricardo Passchier в «BPM – Великая Вавилонская путаница». Даже такой корифей в этой области профессор Шеер путается в определениях и назначении ARIS (один из лидеров систем в области управления процессами).

На мой взгляд построение бизнес процессов – это правильно. Подход типа – купим BPM/BPPM/BPMS/BPA/SEM..., наберем студентов отличников и все у нас будет великолепно – ересь. Для описания бизнес процессов компании любой сложности необходимо три инструмента: карандаш, бумага и голова. Если с первые два компонента в компаниях в избытке, то с третьим обычно наблюдается постоянная нехватка. Основной компонент – люди, работающие в данной сфере, имеющий как теоретическую базу, так и практический опыт в той или иной области бизнеса. Наибольший эффект от коллективной работы сотрудников как «вертикальной» (разные уровни иерархии), так и «горизонтальной» (сотрудники различных подразделений) составляющей организации. Первый этап – перенос на бумагу того, что имеем или создаем. Визуальное отображение процесса помогает лучше понять все аспекты его деятельности. Так же это поможет ИТ перенести процессы на язык машин. На начальном этапе можно использовать любое офисное приложение или бесплатное решение, которое позволяет «рисовать квадратики и кружочки». Все. Далее внедряем, непрерывно отслеживаем результат и вносим изменения.

Специфическое программное обеспечение может понадобится в дальнейшем, при росте количества процессов, их повторное использование и т.п. Кроме этого ряд информационных систем (ERP) имеет в своем функционале графические редакторы или программные средства, позволяющие моделировать бизнес процессы и выполнять их. Некоторые решения умеют «читать» бизнес процесс (файл определённого формата), и мгновенно использовать его. Так на пример Microsoft System Center 2016 имеет возможность моделировать процессы

(в собственном встроенном редакторе) и исполнять его. При этом нет необходимости в разработчиках ПО. Все это упрощает и ускоряет время реакции компании на изменения рынка.

Концепция Информационных Систем и Интеграция данных

Общие Положения

В данной главе книги рассмотрены основные концепции построения Информационных Систем Управления, модели построения интеграции данных. Сделан акцент на Автоматизированные (Информационные) Системы Управления (АСУ), рассмотрены вопросы выбора, внедрения и сопровождения бизнес – ориентированных приложений и решений, как с точки зрения видения бизнеса, так и ее проекция на ИТ инфраструктуру организации. Бизнес приложения являются на мой взгляд вершиной пирамиды построения информационных систем организации, на внедрение и сопровождение которых направлена основная деятельность ИТ департамента. Все технические ИТ сервисы призваны обеспечить работу бизнес приложений.

Информационные Системы Управления (Management Information System MIS) является общим, собирательным термином, которая охватывает информационные системы широкой категорией, имеющиеся в компании, на основе которой руководство компании может организовать коммерческую или иную бизнес деятельность и принимать решения.

Причины появления Автоматизированных Систем Управления (АСУ)

Рассмотрим для примера работу небольшой компании по продаже бананов. Имеется штат офисных сотрудников каждый из которых выполняет свои функциональные обязанности: менеджер по продажам ведет учет покупателей, логистик – учет доставки, бухгалтер – учет и т.п. У каждого из есть компьютер с установленным офисным приложением, например, Microsoft Excel – «убийца ERP систем». Подразумевается навыки хорошего владения продуктом, что для бухгалтеров «старой закалки» являлось нормой. У тех, чей уровень знания Excel ниже, локально на компьютере установлена подходящая программа. Ведение учета, построение сложной аналитики, предоставление отчетов руководству. Помощник руководителя, собирает отчеты у менеджеров, формирует консолидированные отчеты и отправляет руководству. Пересчитать себестоимость по FIFO или LIFO, придумать новую формулу расчета скидок, сценарии продаж и т.п. – «без проблем»: быстро, не дорого и правильно. Не одна ERP с целым штатом консультантов, на мощных серверах и огромными расходами не сможет быстрее и правильнее. Все идет прекрасно, контора растет, до того момента пока:

- один человек перестает справляться, и требуется совместное редактирование Excel файлов двум и более сотрудникам
- Возможности Excel ограничены
- Потребность в скорости обмена актуальными данными возрастает

Минусы автономной работы стали перевешивать плюсы и тормозить бизнес. Нужно что-то делать?

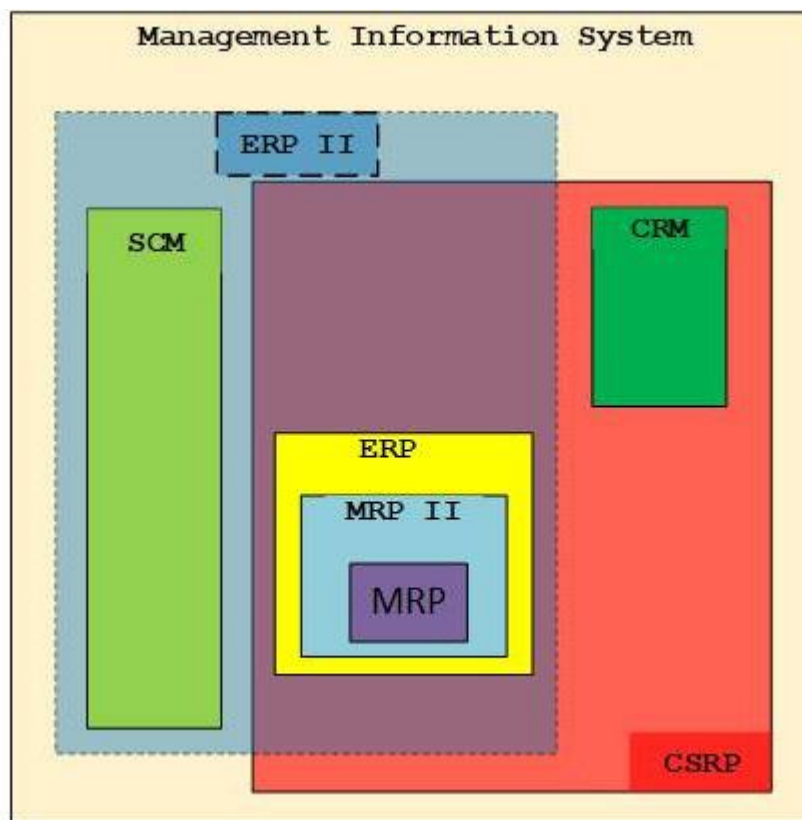
Потребность в автоматизации управленческих процессов впервые была осознана в конце 60-х – начале 70-х годов, когда стало ясно, что управление крупной корпорацией подчиняется тем же законам, что и любая бюрократическая структура. Один из законов Паркинсона гласит: «штат организации никак не связан с объемом выполняемой ею работы». Иными словами, с ростом численности управленческого персонала КПД его работы падает до нуля.

В связи с этим родилась идея: организовать труд управленцев при помощи автоматизированной системы примерно так, как конвейер организует труд рабочих. В итоге родилась концепция регулярного менеджмента, опирающегося не на талантливых одиночек, а на формально описанные процедуры, делающие эффективным труд каждого управленца.

Категории Информационных Систем Управления (Management Information Systems)

Назначение Автоматизированных Систем Управления:

- Обеспечить руководство инструментами, помогающими в принятии решений стратегического, тактического и оперативного управления.
- Обеспечить бизнес подразделения организации инструментами, ведения коммерческой, хозяйственной и прочей деятельности в соответствии с их функциональными задачами.



Основные термины и определения приводятся в Словаре APICS. Именно в этом издании содержится наиболее полное и точное определения систем:

MPS (Master Planning Schedule)

Хорошо известная методология «объемно-календарного планирования». Является базовой практически для всех планово-ориентированных методологий. Применяется в основном в производстве, но также может использоваться и в других отраслях бизнеса, например, дистрибуции.

MRP (Material Requirements Planning) – Автоматизированное планирование потребности сырья и материалов для производства

Методология планирования потребности в материальных ресурсах, заключающаяся в определении конечной потребности в ресурсах по данным объемно-календарного плана производства. Ключевым понятием методологии является понятие «разузлование», т. е. приведение древовидного состава изделия к линейному списку (Bill of Materials), по которому планируется потребность и осуществляется заказ комплектующих. Ее усовершенствованная версия, Closed Loop MRP (планирование потребности в материалах в замкнутом цикле), позволила динамически корректировать планы закупок при возникновении нештатных отклонений от них.

CRP (Capacity Requirements Planning) – Планирование производственных ресурсов

Данная концепция схожа с MRP, но вместо единого понятия состава изделия она оперирует такими понятиями, как «обрабатывающий центр», «машина», «рабочие ресурсы», ввиду чего технически реализация CRP более сложна. Обычно применяется совместно с MRP ввиду тесной логической связи при планировании. Методологии MRP/CRP применяются в АСУП производственных предприятий.

FRP (Finance Requirements Planning) – Планирование финансовых ресурсов

MRP II (Manufacturing Resources Planning)

Планирование и управление всеми производственными ресурсами предприятия:

- сырьем,
- материалами,
- оборудованием,
- трудозатратами.
- Планирование производства.

Интегрированная методология, включающая MRP/CRP и, как правило, MPS и FRP. При использовании данной методологии обязательно подразумевается анализ финансовых результатов производственного плана. Устраняет серьезный недостаток MRP: суть которого в том, что, рассчитывая потребность в материалах, не учитываются производственные мощности, их загрузку, стоимость рабочей силы и т. д. Концепция MRP II позволял планировать все производственные ресурсы предприятия (сырье, материалы, оборудование, персонал и т. д.). Впоследствии концепция MRP II развивалась, и к ней постепенно добавлялись возможности по учету остальных затрат предприятия – появилась концепция ERP (Enterprise Resource Planning – Планирование ресурсов предприятия), называемая иногда также планированием ресурсов в масштабе предприятия (Enterprise-wide Resource Planning).

Развитием концепций автоматизированного управления занимается американская некоммерческая организация APICS (American Production and Inventory Control Society). По стандарту APICS, MRP II включает следующие функции:

- Планирование продаж и производства
- Управление спросом
- Составление плана производства
- Планирование потребностей в сырье и материалах
- Bill of Materials – Спецификации продукции
- Inventory Transaction Subsystem – Складская подсистема
- Отгрузка готовой продукции
- Управление производством на цеховом уровне
- Планирование производственных мощностей
- Input/output control – Контроль входа/выхода
- Purchasing – Материально-техническое снабжение
- Планирование запасов сбытовой сети
- Планирование и управление инструментами
- Financial Planning – Финансовое планирование
- Simulation – Моделирование
- Performance Measurement – Оценка результатов

Задачей информационных систем класса MRP II является оптимальное формирование потока материалов (сырья), полуфабрикатов (в том числе находящихся в производстве) и готовых изделий. Система класса MRP II – имеет целью интеграцию всех основных процессов, реализуемых предприятием, таких как снабжение, запасы, производство, продажа и распространение, планирование, контроль за выполнением плана, затраты, финансы, основные средства и т. д. Стандарт MRP II делит сферы отдельных функций (процедур) на два уровня:

- Необходимый
- Опциональный

Для того, чтобы программное обеспечение было отнесено к классу MRP II, оно должно выполнять определенный объем необходимых (основных) функций (процедур). Некоторые поставщики ПО приняли различный диапазон реализаций опциональной части процедур этого стандарта. Результаты использования интегрированных систем стандарта MRP II:

- получение оперативной информации о текущих результатах деятельности предприятия как в целом, так и с полной детализацией по отдельным заказам, видам ресурсов, выполнению планов;
- долгосрочное, оперативное и детальное планирование деятельности предприятия с возможностью корректировки плановых данных на основе оперативной информации;
- решение задач оптимизации производственных и материальных потоков;
- реальное сокращение материальных ресурсов на складах;
- планирование и контроль за всем циклом производства с возможностью влияния на него в целях достижения оптимальной эффективности в использовании производственных мощностей, всех видов ресурсов и удовлетворения потребностей заказчиков;
- автоматизация работ договорного отдела с полным контролем за платежами, отгрузкой продукции и сроками выполнения договорных обязательств;
- финансовое отражение деятельности предприятия в целом;
- значительное сокращение непроизводственных затрат;
- защита инвестиций, произведенных в информационные технологии;
- возможность поэтапного внедрения системы, с учетом инвестиционной политики конкретного предприятия.

В основу MRP II положена иерархия планов. Планы нижних уровней зависят от планов более высоких уровней, т. е. план высшего уровня предоставляет входные данные, намечаемые показатели и/или какие-то ограничительные рамки для планов низшего уровня. Кроме того, эти планы связаны между собой таким образом, что результаты планов нижнего уровня оказывают обратное воздействие на планы высшего уровня. Если результаты плана нереалистичны, то этот план или планы высшего уровня должны быть пересмотрены. Таким образом можно проводить координацию спроса и предложения ресурсов на определенном уровне планирования и ресурсов на высших уровнях планирования.

ERP (Enterprise Resources Planning) – Управление ресурсами предприятия

К свойствам MRPII добавилось управление финансовыми ресурсами, маркетинг. ERP концепция – первая направленная на управление бизнесом, а не только производства, как MRP. Концепция бизнес-планирования. Под ERP подразумевается «интегрированная» система, выполняющая функции, предусмотренные концепциями MPS-MRP/CRP-FRP. Важным отличием от методологии MRPII является возможность «динамического анализа» и «динамического изменения плана» по всей цепочке планирования. Конкретные возможности методологии ERP существенно зависят от программной реализации. Концепция ERP более «размыта», чем MRPII. Если MRPII имеет явно выраженную направленность на производственные компании, то методология ERP оказывается применимой и в торговле, и в сфере услуг, и в финансовой сфере. Класс ERP, в отличие от MRP и MRP II, для которых имеются строгие определения

и формализованные перечни требований, описан только на уровне концепции. Поэтому утверждения о том, что-то-такая-то система относится к классу ERP, строго говоря, является рекламным утверждением, или, в лучшем случае, экспертным заключением.

В основе ERP лежит концепция ERP: принцип создания единого хранилища данных (repository), содержащего всю деловую информацию, накопленную организацией в процессе ведения деловых операций, включая финансовую информацию, данные, связанные с производством, управлением персоналом, или любые другие сведения. Это устраняет необходимость в передаче данных от системы к системе. Кроме того, любая часть информации, которой располагает данная организация, становится одновременно доступной для всех работников, обладающих соответствующими полномочиями. Концепция ERP стала очень известной в производственном секторе, поскольку планирование ресурсов позволило сократить время выпуска продукции, снизить уровень товарно-материальных запасов, а также улучшить обратную связь с потребителем при одновременном сокращении административного аппарата. Стандарт ERP позволил объединить все ресурсы предприятия, таким образом, добавляя управление заказами, финансами и т. д. Когда в список учитываемых при планировании ресурсов добавились другие, в частности, финансовые, появился термин ERP (Enterprise Resource Planning) – планирование ресурсов в масштабе предприятия.

Различие между концепциями MRP II и ERP заключается в том, что первая ориентирована на производство, а вторая – на бизнес. Например, такие вещи, как условия кредитования заказчика по отгрузке готовой продукции, попадают в поле зрения ERP, но не MRP II. Инструментарий OLAP, средства поддержки принятия решений – принадлежности ERP, но не MRP/MRP II систем.

В соответствии со Словарем APICS, термин «ERP-система» может употребляться в двух значениях:

- информационная система для идентификации и планирования всех ресурсов предприятия, которые необходимы для осуществления продаж, производства, закупок и учета в процессе выполнения клиентских заказов.
- методология эффективного планирования и управления всеми ресурсами предприятия, которые необходимы для осуществления продаж, производства, закупок и учета при исполнении заказов клиентов в сферах производства, распространения и оказания услуг.

Большинство современных ERP-систем построены по модульному принципу, что дает заказчику возможность выбора и внедрения лишь тех модулей, которые ему действительно необходимы. Модули разных ERP-систем могут отличаться как по названиям, так и по содержанию. Тем не менее, есть некоторый набор функций, который может считаться типовым для программных продуктов класса ERP. Такими типовыми функциями являются:

- ведение конструкторских и технологических спецификаций. Такие спецификации определяют состав конечного изделия, а также материальные ресурсы и операции, необходимые для его изготовления (включая маршрутизацию);
- управление спросом и формирование планов продаж и производства. Эти функции предназначены для прогноза спроса и планирования выпуска продукции;
- планирование потребностей в материалах. Позволяют определить объемы различных видов материальных ресурсов (сырья, материалов, комплектующих), необходимых для выполнения производственного плана, а также сроки поставок, размеры партий и т. д.;
- управление запасами и закупочной деятельностью. Позволяют организовать ведение договоров, реализовать схему централизованных закупок, обеспечить учет и оптимизацию складских запасов и т. д.;
- планирование производственных мощностей. Эта функция позволяет контролировать наличие доступных мощностей и планировать их загрузку. Включает укрупненное планирование мощностей (для оценки реалистичности производственных планов) и более детальное планирование, вплоть до отдельных рабочих центров;
- финансовые функции. В эту группу входят функции финансового учета, управленческого учета, а также оперативного управления финансами;

•функции управления проектами. Обеспечивают планирование задач проекта и ресурсов, необходимых для их реализации.

ERP не является вершиной эволюции. Фундаментальное ограничение систем ERP: они автоматизируют внутреннюю деятельность предприятия так называемый «back-office».

CSRP (Customer Synchronized Resources Planning) – Управление, ориентированное на взаимодействие с клиентами

Управление, ориентированное на взаимодействие с клиентами, включает в себя получение заказов, разработку планов, проектов и заданий, техподдержку. Практически, CSRP=ERP+CRM. Планирование ресурсов, синхронизированное с покупателем. CSRP включает в себя полный цикл – от проектирования будущего изделия с учетом требований заказчика, до гарантийного и сервисного обслуживания после продажи. Суть CSRP состоит в том, чтобы интегрировать покупателя в систему управления предприятием. При этом не отдел продаж, а сам покупатель размещает заказ на изготовление продукции, сам отвечает за правильность его исполнения и при необходимости отслеживает соблюдение сроков производства и поставки. Предприятие же может очень четко отслеживать тенденции спроса на его продукцию.

Концепция CSRP – Customer Synchronized Resource Planning (Планирование ресурсов, синхронизированное с покупателем) – охватывает также и взаимодействие с клиентами: оформление наряд-заказа, тех задание, поддержка заказчика на местах и пр. Таким образом, если MRP, MRP-II, ERP ориентировались на внутреннюю организацию предприятия, то CSRP включил в себя полный цикл от проектирования будущего изделия, с учетом требований заказчика, до гарантийного и сервисного обслуживания после продажи. Основная суть концепции CSRP в том, чтобы интегрировать Заказчика (Клиента, Покупателя и пр.) в систему управления предприятием. То есть не отдел сбыта, а сам покупатель непосредственно размещает заказ на изготовление продукции – соответственно сам несет ответственность за его правильность, сам может отслеживать сроки поставки, производства и пр. При этом предприятие может очень четко отслеживать тенденции спроса и т. д. На расширение функциональности на сферу взаимодействия предприятия с его заказчиками нацелена концепция CSRP. Корпоративные ресурсы, охватываемые CSRP-системой, обслуживают такие этапы производственной деятельности, как проектирование будущего изделия с учетом специфических требований заказчика, гарантийное и сервисное обслуживание.

CSRP – это первая бизнес методология, которая интегрирует деятельность предприятия, ориентированную на покупателя, в центр системы управления бизнесом. CSRP устанавливает методологию ведения бизнеса, основанную на текущей информации о покупателе. CSRP сдвигает фокус предприятия с планирования от потребностей производства к планированию от заказов покупателей. Информация о покупателях и услуги встраиваются в основу организации. Деятельность по производственному планированию не просто расширяется, а удаляется и заменяется запросами покупателей, переданными из подразделений организации, ориентированных на работу с покупателями. CSRP переопределяет практику бизнеса, фокусируя ее на рыночной активности, а не на производственной деятельности. Бизнес-процессы синхронизируются с деятельностью покупателей.

CSRP переопределяет обслуживание покупателей и расширяет его за пределы обычной телефонной поддержки и выдачи справки о счетах. При использовании модели CSRP покупательские услуги становятся спинным мозгом целого предприятия, командным пунктом для организации. Центр технической поддержки покупателей отвечает за доведение критической информации о покупателях к исполнительным центрам организации. Выгоды успешного применения CSRP – это повышение качества товаров, снижение времени поставки, повышение ценности продуктов для покупателя и так далее, а в результате этого – снижение производственных издержек, но что более важно, это создание инфраструктуры, приспособленной для создания продуктов, удовлетворяющих потребности покупателя,

улучшение обратной связи с покупателями и обеспечение лучших услуг для покупателей. Это не эффективность производства, которая будет обеспечивать временные конкурентные преимущества, скорее это способность создавать продукты, удовлетворяющие потребности покупателя и лучший сервис. Способность создавать покупательскую ценность приведет к росту доходов и устойчивому конкурентному преимуществу.

При использовании модели бизнеса CSRP, традиционные бизнес-процессы пересматриваются в направлении к обслуживанию покупателей и созданию продуктов, удовлетворяющих их потребности. Внедрение приложений CSRP подталкивает руководителей предприятия к изменению. Внутренняя сфокусированность традиционных производственных структур, сегментированная по отделам и функциональности, перефокусируется наружу. CSRP позволяет построить двунаправленный свободный поток информации между покупателем и производителем.

ERP II (Enterprise Resource and Relationship Processing) – Управление внутренними ресурсами и внешними связями предприятия

Новая ревизия концепции ERP. Можно считать, что, $ERP II = ERP + CRM + SCM$. Пока что данный класс применяется нечасто. Основная идея ERP II заключается в выходе за рамки задач по оптимизации внутренних процессов организации: кроме интеграции таких традиционных для ERP систем областей деятельности предприятия, как управление финансами, бухгалтерский учет, управление продажами и покупками, отношения с дебиторами и кредиторами, управление персоналом, производство, управление запасами, системы класса ERP II позволяют управлять взаимоотношениями с клиентами, цепочками поставок, вести торговлю через Интернет. По определению, данному Gartner Group ERP II, – это бизнес-стратегия предприятия, принадлежащего к определенной отрасли, и набор ключевых для данной отрасли приложений, помогающих клиентам и акционерам компаний увеличивать стоимость бизнеса за счет эффективной ИТ-поддержки и оптимизации операционных и финансовых процессов как внутри своего предприятия, так и во внешнем мире – в рамках сотрудничества с другими корпорациями. Основная идея ERP II заключается в выходе за рамки задач по оптимизации внутренних процессов организации: кроме интеграции таких традиционных для ERP систем областей деятельности предприятия, как управление финансами, бухгалтерский учет, управление продажами и покупками, отношения с дебиторами и кредиторами, управление персоналом, производство, управление запасами, системы класса ERP II позволяют управлять взаимоотношениями с клиентами, цепочками поставок, вести торговлю через Интернет. Функции и преимущества систем, которые реализованы в ERP II:

- Управление взаимоотношениями с клиентами (CRM).
- Управление послепродажным обслуживанием клиентов.
- Электронная коммерция.

Новая функциональность ERP II, позволяет эффективно управлять контактами с клиентами, рекламными кампаниями, сбытом, проводить маркетинговые исследования. Это достигается за счет создания персональных профилей клиентов, классификации клиентов по различным категориям, определения целевых групп для рекламных кампаний, планирования и контроля взаимодействия с клиентами (телефонные звонки, визиты, рассылка рекламных и маркетинговых материалов и т. д.), упрощенного доступа к данным о существующих и потенциальных клиентах, поставщиках. Существует также возможность тарифицировать различные типы контактов и точно оценивать затраты на проведение различных мероприятий. Благодаря интеграции с другими подсистемами появляется возможность сопоставления с результатов маркетинговых кампаний с фактическими данными продаж. Это позволяет повысить координацию работы служб маркетинга, сбыта и снабжения.

Сервисным подразделениям система дает возможность организовать эффективное управление послепродажным обслуживанием клиентов. Функциональные средства позволяют

регистрировать действия, осуществляемые компанией после продажи товаров. При этом заявки на сервисное обслуживание могут быть инициированы как самими клиентами, так и автоматически, согласно сервисному контракту. Данные в сервисный заказ могут быть внесены как сотрудником, принявшим звонок, так и работником сервисной службы. В системе имеется возможность определять приоритетные сервисные заказы и загрузку персонала, выбирать персонал и работников технической службы по их занятости, профессиональной ориентации. Проанализировав исторические данные о сервисных работах можно выявлять наиболее «слабые места» в производимой продукции. Интеграция с подсистемой управления запасами позволяет при приеме заказа на сервисное обслуживание выяснить наличие запасных частей, а в случае их отсутствия определить сроки поступления на склад или зарегистрировать заявку на приобретение. Клиент в любой момент может проследить, как выполнялся заказ и его статус.

Электронная коммерция. Для продвижения своего бизнеса в Интернет необходимо, прежде всего, выстроить и отработать свои бизнес процессы до открытия Интернет представительства. Отсутствие «надежного тыла» становится серьезной проблемой для компании. Это обусловлено тем, что при обычной схеме работы задача часто решается следующим образом: создается каталог продукции с описанием товаров и интерактивной формой заказа, клиент заказывает товар и ждет его доставки. Однако зачастую, осуществляя заказ, клиент, да и сами менеджеры, не имеют понятия, есть ли товар на складе и в случае отсутствия, сколько времени понадобится, чтобы доставить товар на склад, а затем переправить его клиенту. Более того, если единожды компания осуществляла специальный заказ для клиента, данные об этом не сохраняются, и при вторичном заказе компания вновь обрабатывает его как новый. Это приводит к простоям, затягивает сроки доставки заказов, что, в конечном счете, влечет за собой полное разочарование клиентов. Функциональность систем ERP II, в свою очередь, позволяют контролировать склад, закупки и поставки и организовывать систему работы оптимальным образом. Помимо оптимизации рабочих процессов, решения ERP II позволяет создать клиентскую базу, хранить и анализировать данные по предпочтениям. Компания также получают возможность прогнозировать сроки последующих заказов постоянных покупателей и предоставлять более персонализированный сервис, что служит выработке приверженности покупателей к сотрудничеству и установлению длительных отношений с клиентами. Таким образом, использование ERP-систем при ведении электронной торговли позволяет компаниям добиться преимущества по отношению к конкурентам. С появлением на рынке систем ERP II, ориентированных на средние предприятия, компании получают возможность развивать торговые площадки в Интернет, которые оптимально будут отвечать их нуждам – обеспечивать электронный документооборот, контролировать движение заказов и т. д. Это позволит компаниям использовать свои Интернет – ресурсы для взаимодействия с поставщиками или дистрибьюторами. Использование систем класса ERP II в данном случае позволяет оптимизировать процессы, как закупок, так и продаж. Информация о заказах, полученных через Интернет, интегрируется с данными склада, отделов доставки, продаж, сервисных центров, что позволяет создать единый профиль клиента, эффективно обрабатывать заказы и быстро отвечать на них, создавать и хранить данные обо всех его обращениях, анализировать их и прогнозировать новые обращения. Клиент, в свою очередь, отправив заказ через Интернет – представительство, получает возможность контролировать процесс обработки заказа: автоматическое уведомление о его принятии и начале работы, данные о подготовке заказа, когда его заявка получена складом, сведения об отгрузке, когда заказ сформирован и отправлен, а также пакет необходимых документов. Аналогично используется система при закупках. Менеджер по закупкам через систему получает доступ к каталогу товаров поставщика, выбирает необходимые товары и отправляет заказ. Возможны варианты, когда система автоматически формирует заказ на покупку, учитывая оптимальные объемы закупок, текущие потребности, необходимые сроки поставки и в стандартном формате пересылает поставщику. Система у поставщика обрабатывает полученный заказ, вычисляет срок поставки и посылает уведомление о ходе выполнения заказа.

SCM (Supply Chain Management) – Управление отношениями с поставщиками

Управление цепочками поставок. Концепция SCM придумана для оптимизации управления логистическими цепями и позволяет существенно снизить транспортные и операционные расходы путем оптимального структурирования логистических схем поставок. Концепция SCM поддерживается в большинстве систем ERP- и MRPII-класса.

CRM (Customer Relationship Management) – Управление отношениями с заказчиками

Отслеживание истории развития взаимоотношений, координировать многосторонние связи, централизованно управлять продажами и клиент-ориентированным маркетингом. Концепция построения автоматизированных систем обслуживания клиентов компании. CRM подразумевает накопление, обработку и анализ не только финансово-бухгалтерской, но и прочей информации о взаимоотношениях с клиентами. Это способствует повышению производительности менеджеров, улучшает качество обслуживания клиентов и способствует увеличению продаж.

PLM (Product Lifecycle Management) – управление жизненным циклом продукта

CAD/CAM/CAE/PDM (Computer-Aided Design/ Computer-Aided Manufacturing/ Computer-Aided Engineering/ Project Data Management) – автоматизированные системы: проектирования/ технологической подготовки производства/ инженерных расчетов/ документооборота

MES (Manufacturing Execution System) Система управления производственными процессами

Специализированное прикладное программное обеспечение, предназначенное для решения задач синхронизации, координации, анализа и оптимизации выпуска продукции в рамках какого-либо производства. Существует несколько формулировок определения MES систем. MES – информационная и коммуникационная система производственной среды предприятия (определение APICS). MES – автоматизированная система управления и оптимизации производственной деятельности, которая в режиме реального времени: иницирует, отслеживает, оптимизирует, документирует производственные процессы от начала выполнения заказа до выпуска готовой продукции (определение MESA International). MES – интегрированная информационно-вычислительная система, объединяющая инструменты и методы управления производством в реальном времени. MES-системы относятся к классу систем управления уровня цеха, но могут использоваться и для интегрированного управления производством на предприятии в целом. Функции с-MES:

- RAS (Resource Allocation and Status) – контроль состояния и распределение ресурсов.
- DPU (Dispatching Production Units) – диспетчеризация производства (координация изготовления продукции).
- DCA (Data Collection/Acquisition) – сбор и хранение данных.
- LUM (Labor/User Management) – управление людскими ресурсами.
- QM (Quality Management) – управление качеством.
- PM (Process Management) – управление процессами производства.
- PTG (Product Tracking & Genealogy) – отслеживание и генеалогия продукции.
- PA (Performance Analysis) – анализ эффективности.
- Advanced Planning & Scheduling (APS) – составления производственных расписаний в рамках всего предприятия,
- Enterprise Asset Management (EAM) – отвечает за управление техническим обслуживанием и ремонтами.

В зависимости от характера, масштаба и особенностей производственных структур и самих систем, существуют различные комбинации сочетаний корпоративных систем ERP, APS и MES в общей структуре информационных систем управления предприятием.

SCADA (Supervisory Control and Data Acquisition System) – система сбора данных и оперативного диспетчерского управления технологических процессов

Хотелось бы подчеркнуть, что в названии присутствуют две основные функции, возлагаемые на SCADA_систему:

- сбор данных о контролируемом технологическом процессе;
- управление технологическим процессом, реализуемое ответственными лицами на основе собранных данных и правил (критериев), выполнение которых обеспечивает наибольшую эффективность и безопасность технологического процесса.

B2C (Business to Customer) и B2B (Business to Business)

обозначения широких классов программных продуктов, обслуживающих взаимоотношения предприятий с покупателями (B2C) и между собой (B2B). Пример B2C-системы – онлайн-интернет-магазин. К классу B2B относятся SCM и CSRP-решения. Технологии B2B в настоящее время переживают настоящий бум. Аналитики соревнуются в предсказании астрономических сумм, которые будут потрачены на них в ближайшие годы. Этот бум связан с вступлением развитых стран в постиндустриальный период. Во все больших масштабах крупные корпорации стремятся избавляться от производства, оставляя за собой исследования, проектирование, маркетинг и продажи. Производство же размещается на фабриках, расположенных в странах с дешевой рабочей силой, и являющихся независимыми предприятиями-подрядчиками. Понятно, что такая схема ведения бизнеса невозможна без совершенных B2B-систем.

OLAP (Online Analytical Processing – аналитическая обработка данных в реальном времени)

Представляет собой мощную технологию обработки и исследования данных. Системы, построенные на основе технологии OLAP, предоставляют практически безграничные возможности по составлению отчетов, выполнению сложных аналитических расчетов, построению прогнозов и сценариев, разработке множества вариантов планов. В основе работы OLAP системы лежит обработка многомерных массивов данных. Многомерные массивы устроены так, что каждый элемент массива имеет множество связей с другими элементами. Чтобы сформировать многомерный массив, OLAP система должна получить исходные данные из других систем (например, ERP или CRM системы), или через внешний ввод. Пользователь OLAP системы получает необходимые данные в структурированном виде в соответствии со своим запросом. Исходя из указанного порядка действий, можно представить структуру OLAP системы. В общем виде, структура OLAP системы состоит из следующих элементов:

- База данных является источником информации для работы OLAP системы. Вид базы данных зависит от вида OLAP системы и алгоритмов работы OLAP сервера. Как правило, используются реляционные базы данных, многомерные базы данных, хранилища данных и т. п.

- OLAP сервер. Он обеспечивает управление многомерной структурой данных и взаимосвязь между базой данных и пользователями OLAP системы.

- Пользовательские приложения. Этот элемент структуры OLAP системы осуществляет управление запросами пользователей и формирует результаты обращения к базе данных (отчеты, графики, таблицы и пр.)

В зависимости от способа организации, обработки и хранения данных, OLAP системы могут быть реализованы на локальных компьютерах пользователей или с использованием выделенных серверов. Существует три основных способа хранения и обработки данных:

- локально. Данные размещаются на компьютерах пользователей. Обработка, анализ и управление данными выполняется на локальных рабочих местах. Такая структура OLAP системы имеет существенные недостатки, связанные со скоростью обработки данных, защищенностью данных и ограниченным применением многомерного анализа.

- реляционные базы данных. Эти базы данных используются при совместной работе OLAP системы с CRM системой или ERP системой. Данные хранятся на сервере этих систем в виде реляционных баз данных или хранилищ данных. OLAP сервер обращается к этим базам данных для формирования необходимых многомерных структур и проведения анализа.

- многомерные базы данных. В этом случае данные организованы в виде специального хранилища данных на выделенном сервере. Все операции с данными осуществляются на этом сервере, который преобразует исходные данные в многомерные структуры. Такие структуры называют OLAP кубом. Источниками данных для формирования OLAP куба являются реляционные базы данных и/или клиентские файлы. Сервер данных осуществляет предварительную подготовку и обработку данных. OLAP сервер работает с OLAP кубом, не имея непосредственного доступа к источникам данных (реляционным базам данных, клиентским файлам и др.).

В зависимости от метода хранения и обработки данных, все OLAP системы могут быть разделены на три основных вида:

- ROLAP (Relational OLAP – реляционные OLAP системы) – этот вид OLAP системы работает с реляционными базами данных. Обращение к данным осуществляется напрямую в реляционную базу данных. Данные хранятся в виде реляционных таблиц. Пользователи имеют возможность осуществлять многомерный анализ как в традиционных OLAP системах. Это достигается за счет применения инструментов SQL и специальных запросов. Одним из преимуществ ROLAP является возможность более эффективно осуществлять обработку большого объема данных. Другим преимуществом ROLAP является возможность эффективной обработки как числовых, так и текстовых данных. К недостаткам ROLAP относится низкая производительность (по сравнению с традиционными OLAP системами), т. к. обработку данных осуществляет сервер OLAP. Другим недостатком является ограничение функциональности из-за применения SQL.

- MOLAP (Multidimensional OLAP – многомерные OLAP системы). Этот вид OLAP систем относится к традиционным системам. Отличие традиционной OLAP системы, от других систем, заключается в предварительной подготовке и оптимизации данных. Эти системы, как правило, используют выделенный сервер, на котором осуществляется предварительная обработка данных. Данные формируются в многомерные массивы – OLAP кубы. MOLAP системы являются самыми эффективными при обработке данных, т. к. они позволяют легко реорганизовать и структурировать данные под различные запросы пользователей. Аналитические инструменты MOLAP позволяют выполнять сложные расчеты. Другим преимуществом MOLAP является возможность быстрого формирования запросов и получения результатов. Это обеспечивается за счет предварительного формирования OLAP кубов. К недостаткам MOLAP системы относится ограничение объемов, обрабатываемых данных и избыточность данных, т. к. для формирования многомерных кубов, по различным аспектам, данные приходится дублировать.

- HOLAP (Hybrid OLAP – гибридные OLAP системы). Гибридные OLAP системы представляют собой объединение систем ROLAP и MOLAP. В гибридных системах постарались объединить преимущества двух систем: использование многомерных баз данных и управление реляционными базами данных. HOLAP системы позволяют хранить большое количество данных в реляционных таблицах, а обрабатываемые данные размещаются в предварительно построенных многомерных OLAP кубах. Преимущества этого вида систем заключаются в масштабируемости данных, быстрой обработке данных и гибком доступе к источникам данных.

Существуют и другие виды OLAP систем, но они в большей степени являются маркетинговым ходом производителей, чем самостоятельным видом OLAP системы:

- WOLAP (Web OLAP). Вид OLAP системы с поддержкой web интерфейса. В этих системах OLAP есть возможность обращаться к базам данных через web интерфейс.

- DOLAP (Desktop OLAP). Этот вид OLAP системы дает возможность пользователям загрузить на локальное рабочее место базу данных и работать с ней локально.

- Mobile OLAP. Это функция OLAP систем, которая позволяет работать с базой данных удаленно, с использованием мобильных устройств.

- SOLAP (Spatial OLAP). Этот вид OLAP систем предназначен для обработки пространственных данных. Он появился как результат интеграции географических информационных систем и OLAP системы. Эти системы позволяют обрабатывать данные не только в буквенно-цифровом формате, но и в виде визуальных объектов и векторов.

Применение OLAP системы дает организации возможности по прогнозированию и анализу различных ситуаций, связанных с текущей деятельностью и перспективами развития. Эти системы можно рассматривать как дополнение к системам автоматизации уровня предприятия. Все преимущества OLAP систем напрямую зависят от точности, достоверности и объема исходных данных. Основными преимуществами OLAP системы являются:

- согласованность исходной информации и результатов анализа. При наличии OLAP системы всегда есть возможность проследить источник информации и определить логическую связь между полученными результатами и исходными данными. Снижается субъективность результатов анализа.

- проведение многовариантного анализа. Применение OLAP системы позволяет получить множество сценариев развития событий на основе набора исходных данных. За счет инструментов анализа можно смоделировать ситуации по принципу «что будет, если».

- управление детализацией. Детальность представления результатов может изменяться в зависимости от потребности пользователей. При этом нет необходимости осуществлять сложные настройки системы и повторять вычисления. Отчет может содержать именно ту информацию, которая необходима для принятия решений.

- выявление скрытых зависимостей. За счет построения многомерных связей появляется возможность выявить и определить скрытые зависимости в различных процессах или ситуациях, которые влияют на производственную деятельность.

- создание единой платформы. За счет применения OLAP системы появляется возможность создать единую платформу для всех процессов прогнозирования и анализа на предприятии. В частности, данные OLAP системы, являются основой для построения прогнозов бюджета, прогноза продаж, прогноза закупок, плана стратегического развития и пр.

ABS (Automated Banking System, Core Banking System) Автоматизированная Банковская Программа

Специализированное комплексное программное обеспечение, предназначенное для ведения операционной деятельности в банковской сфере.

Классификация Управления Организацией

Функционально Ориентированная Организация Управления

Суть данной организации управления заключается в том, что перед каждой функциональной структурной единицей организации (бухгалтерия, отдел сбыта, администрация и т п) закреплена ряд функций, описана область ответственности, сформулированы критерии успешной

и неуспешной деятельности. При этом, как правило, данный подход характеризуется следующими выраженными признаками:

- Слабые горизонтальные связи между функциональными структурными единицами,
- Сильные вертикальные линии связи внутри одной функциональной структуры, типа «начальник-подчиненный».

Подчиненный отвечает только за порученные ему функции и, возможно, за деятельность своего подразделения в целом. Функции и результаты работы параллельных структурных единиц его не очень интересуют. Данные структурируются по функциональному назначению структурных подразделений компании. Как пример, для небольшой компании в качестве ИТ решения может быть выбрано решение 1С «Бухгалтерия» для ведения хозяйственной деятельности, бухгалтерского и Управленческого учета. Все остальные функциональные подразделения используют данное решение для автоматизации операционной деятельности исходя из имеющегося функционала. Для крупной компании для финансового департамента может быть выбрано решение, например, Программа 1С конфигурация «Бухгалтерия», а для Отдела Кадров выбрано решение 1С конфигурация «Управление Сотрудниками», отвечающие требованиям подразделений.

Функциональный подход к управлению оптимален для предприятий с простой организационной структурой, когда весь бизнес (или его значительная часть) сосредоточена в рамках одной структурной единицы, или же для крупного предприятия, бизнес процессы которого идут обособленно. Например, в случае промышленного предприятия, когда некоторая структурная единица выполняет полный цикл производства некоторого товара. В целом этот подход больше всего подходит предприятиям со стабильными бизнес-процессами, что присуще, например, предприятиям, действующим на рынках с низким уровнем конкуренции. На данный момент наблюдается преобладает функциональном (иерархическом) подходе к управлению организацией.

Процесс Ориентированная Организация Управления

При процессном подходе к организации управления, каждая структурная единица обеспечивает выполнение конкретных бизнес-процессов, в которых она участвует. Обязанности, область ответственности, критерии успешной деятельности для каждой структурной единицы сформулированы и имеют смысл лишь в контексте конкретного бизнес-процесса. Данный подход как правило характеризуется следующими признаками:

- Горизонтальные связи между структурными единицами при таком подходе сильнее
- Вертикальные слабее, чем в случае функционального подхода.

Сотрудник отвечает не только за свои функции, но и за те бизнес-процессы, в которых он задействован, поэтому результаты деятельности параллельных структурных единиц, которые участвуют в тех же бизнес-процессах, что и он, для него важны.

В контексте управления ИТ сервисами, данные структурируются по назначению процесса бизнес приложений. Как пример, в компании определяются бизнес процессы (процесс закупки, процесс движения денежных средств, и т.п.). В процесс закупки на различных этапах деятельности, вовлечены различные функциональные подразделения организации (например, отдел закупок отвечает за сбор предложений, проведение тендера, финансовый департамент отвечает за оплату, административный отдел за доставку товара и т.п.). Как пример для

Для современных предприятий характерна сложная организационная структура, в рамках которой ответственность за выпуск конечного продукта или услуги распределяется между многими структурными единицами. И в этом случае преимущества процессного подхода становятся очевидны, особенно для предприятий, которым приходится часто изменять свои бизнес-процессы, что характерно для рынков с высоким уровнем конкуренции. Процессный подход позволяет взглянуть на информационную систему не как на программу, на которую приходится расходовать финансы, а как на инструмент бизнеса направленный на получение ценности для компании.

Классификация Информационных Систем с точки зрения ИТ Функционально Ориентированная Информационная Система

Как видно из особенностей функционально ориентированного подхода к управлению организацией, информационная система предприятия выбирается исходя из требований функционального подразделения компании. Так для примера, была выбрана система «1С конфигурация Бухгалтерия» покрывающая требования по ведению Управленческого, Бухгалтерского и Налогового Учета в процессе ведения коммерческой и хозяйственной деятельности. Деятельность остальных подразделений (отдела кадров, отдела продаж, администрации и т.п.) по возможности встраивается в имеющуюся информационную систему с использованием «базового» функционала. В процессе развития компании, информационная система модернизируется, обновляется и в целом удовлетворяет требованиям бизнеса. ИТ департамент обеспечивает внедрение и сопровождение системы. На каком-то этапе своего развития отдел продаж или маркетинга, нуждается в дополнительном функционале, отсутствующем в имеющейся системе. Перед руководством компании, как и перед руководителем ИТ департамента, возникает вопрос: сменить текущую систему на новую, в которой помимо имеющегося функционала, так же присутствуют функции, требуемые со стороны отдела продаж. Бухгалтерия, а возможно и другие подразделения, возможно будут против, как и руководитель ИТ по следующим причинам:

- Текущая система удовлетворяет требования большинства подразделений компании
- Имеется наработанная практика работы с программой со стороны бизнеса
- Имеется наработанная практика работы с программой со стороны ИТ (баги, ошибки, навыки сопровождения и т.п.)

Внедрение новой системы неизбежно ведет к появлению следующих обязательных вопросов:

- Постановка технического задания по имеющимся функциям
- Постановка технического задания по новым функциям
- Реинжиниринг бизнес процессов для адаптации к новой системе
- Наличие ресурсов для внедрения и сопровождения
- Как новое решение вписывается в имеющуюся ИТ инфраструктуру
- План внедрения новой информационной системы без прерывания бизнеса
- План миграции информации из старой системы в новую
- Обучение персонала
- Вопросы по поддержке
- План восстановления бизнеса на случай не удачного внедрения проекта

В независимости от полноты ответов и правильности их реализации, внедрение новой системы неизбежно ведет к появлению следующих потенциальных рисков и проблем:

- Расходы на внедрение новой системы (как прямые, так и косвенные расходы времени и денег)
- Не удобство для пользователей (интерфейс другой, формы и процессы могут отличаться значительно)
- Возрастания количества ошибок и проблем во времени эксплуатации системы пользователями (не знают, ошибки и т.п.)
- Время устранения проблем со стороны ИТ увеличивается (ИТ не имеет навыков по сопровождению системы)
- Вопросы по миграции данных из старой системы в новую

Вообще, как уже упоминалось ранее в книге, для замены текущей системы на новую необходимы очень важные доводы, и это последнее, о чем должен думать ИТ архитектор при построении ИТ Архитектуры Предприятия.

Как результат, скорее всего будет принято решение, по приобретению отдельного решения с имеющимся функционалом, удовлетворяющим требования отдела продаж. Например, Microsoft Navision CRM.

Некоторые *преимущества данного решения* будут:

- Влияние на текущие бизнес процессы минимальный, так как компания продолжает работать с имеющимся решением
- Расходы по внедрению значительно ниже

- Уровень всех потенциальных проблем снижается по причине уменьшения масштаба влияния
- При провале проекта, отдел продаж продолжит работать с имеющейся системой
- Нет необходимости в миграции данных

Но возникают вопросы: Есть ли необходимость технической интеграции двух систем между собой и если да, то как и на каком уровне. Преимущества выбора Функционально Ориентированной Информационной Системы:

- Содержит необходимый функционал для обеспечения работы
- Обычно более проста и понятна для внедрения и использования
- Процесс внедрения проще за счет меньшего масштаба внедрения

Недостатки:

- Сопровождение потенциально большего количества информационных систем
- Вопросы по интеграции большего количества информационных систем между собой
- Требуется большего распыления ИТ ресурсов
- Требования по знанию различных систем

Процесс Ориентированная Информационная Система

Теперь рассмотрим особенности Процесс ориентированного подхода к управлению организацией, и его влияние на построении ИТ инфраструктуры компании. Информационная система предприятия выбирается исходя из анализа бизнес процессов, происходящих в компании. Как написано в предыдущей главе, компания описывает бизнес процессы как основные, так и вспомогательные. Полнота описания процессов и их точность позволит выбрать наиболее правильное решение. Так для примера, была выбрана система «Microsoft Dynamics Navision» или 1С Конфигурация Управление Предприятием» покрывающая требования всех имеющихся бизнес процессов. Также в процессе роста организации могут возникнуть потребности в новом функционале, и требовании интеграции имеющегося решения с новой системой.

Преимущества выбора Процесс Ориентированной Информационной Системы:

- Содержит необходимый функционал для обеспечения работы компании на протяжении всего жизненного цикла
- Сопровождение меньшего количества информационных систем (потенциально единая система в организации)
- Вопрос по интеграции информационных систем между собой не актуален или не критичный
- Не требует распыления ИТ ресурсов
- Нет требований по знанию большого количества различных систем

Недостатки:

- Более высокая первоначальная стоимость решения за счет большего функционала
- Риски внедрения и сопровождения выше, так как является основной для бизнеса, относительно сложной и т п

«Эталонная» Информационная Система (Management Information System)

При анализе и сравнении выше приведенных систем, а также исходя из опыта внедрения и сопровождения различных информационных систем, возможности бизнеса и т п можно создать так называемую идеальную «эталонную» модель Информационной Системы для вашей компании. На мой взгляд, в контексте построения крупной, централизованной Архитектуры Предприятия, идеальная модель будет выглядеть как:

•Единая Универсальная Информационная Система, построенная по модульному принципу, совмещающая в себе как функциональный, так и процессный подходы.

Преимущества Единой Информационной Системы:

- Все преимущества Процесс Ориентированной Информационной Системы

- За счет модульности, первоначальная стоимость внедрения и последующее сопровождение значительно дешевле

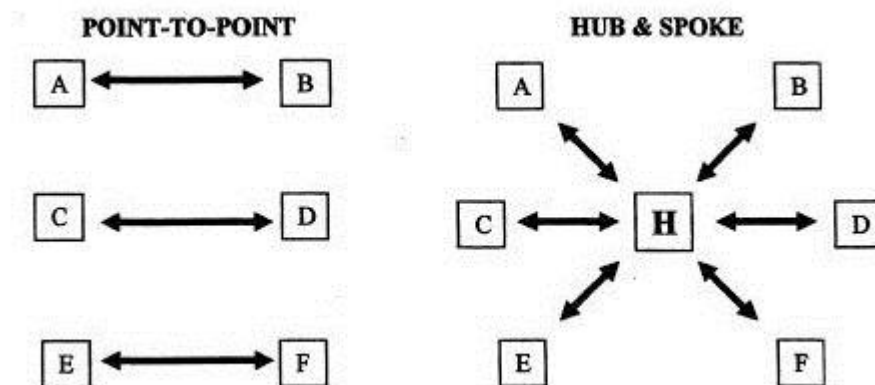
- Так же за счет модульности, дополнительный функционал внедряется по необходимости
- Снижаются риски при внедрении и сопровождении нового функционала
- Единая информационная система от одного производителя более надежна, безопаснее и управляема

Все хорошо, ясно и понятно, руководитель компании вызывает к себе, ставит задачу найти «самое-самое» решение. Ищем, внедряем и спим спокойно дорогой товарищ. Но как говорится «... если хотите получить чудо – нанимайте сказочников...». На практике, любое более-менее среднее или тем более большое предприятие с более или менее тесной интеграцией с ИТ имеет в своем «зоопарке» два и более ИТ бизнес решения. Это связано с тем, что в каждой бизнес сфере (финансовая сфера, банках, страховых компаниях, строительстве, сельском хозяйстве и т п) имеется своя особенность ведения бизнеса. Кроме этого для международных компаний требования законодательства для одних и тех же функциональных подразделений может различаться кардинально. Адаптация или переделка «универсального» решения может быть очень трудоемким, затратным и провальным проектом. Не изобретайте велосипед заново там, где в этом нет особой необходимости.

Модели Интеграции Информационных Систем

Общая модель интеграции данных и информационных поток представлена на диаграмме. Как видно из диаграмм различают основные модели интеграции систем:

«Точка – точка» (*Point-to-point*) наиболее простая модель, использует прямое соединение систем между собой



Модель интеграции типа «Point-to-point» и «Hub & Spoke»

«ХАБ» (*Hub & Spoke*) представляется в виде центрального элемента, соединенного с различными системами

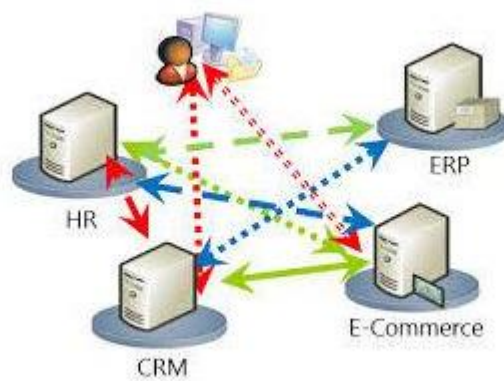


Диаграмма Модели интеграции типа «Spaghetti»

«ЛЕС» (*Spaghetti*) – модель соединения всех систем со всеми
 «Интеграционная Шина Предприятия» (Enterprise Service Bus) общая «шина» данных для интеграции систем между собой, представляет из себя как правило самостоятельную систему.

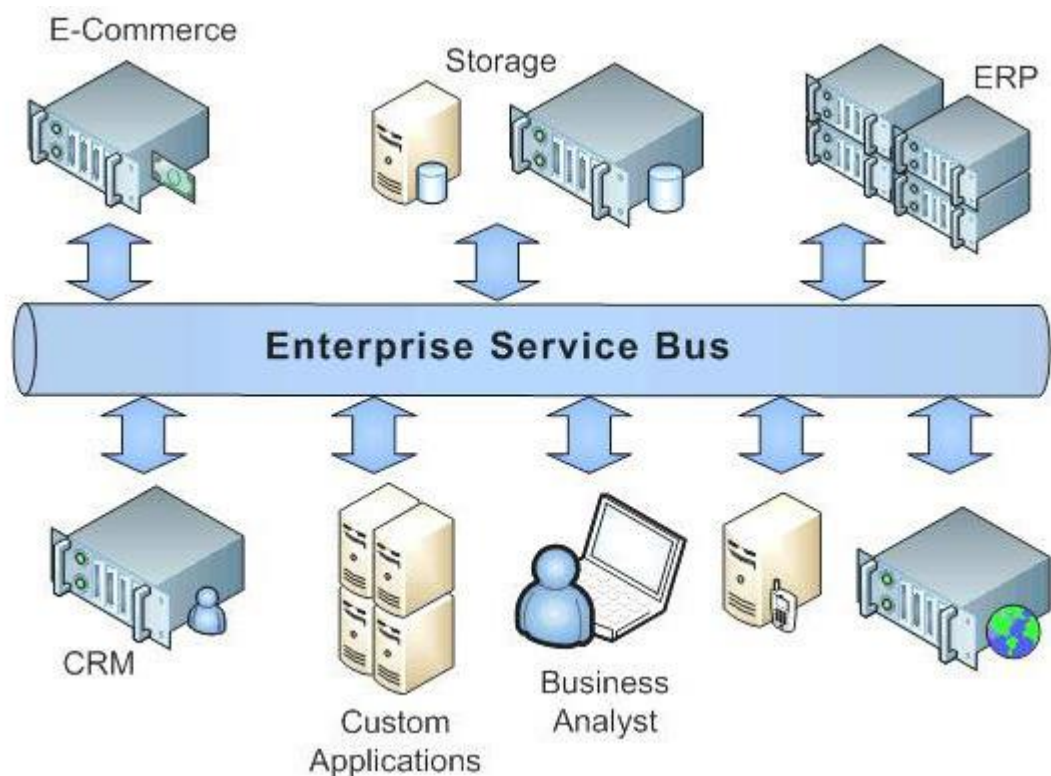


Диаграмма Модели интеграции типа «Enterprise Service Bus»

Далее компоненты систем интеграции можно разделить на следующие элементы:

- Периферийные системы (Front-end) – решения специфической операционной деятельности, или требует установку локально для взаимодействия с различными аппаратными решениями на местах (станки, кассовые аппараты и т п)
- Механизм интеграции данных (Integration) – механизмы интеграции данных

- Ключевые системы (Back-end) – конечные системы, решение консолидации и обработки данных
- Системы консолидации (OLAP & BI) – решение консолидированной аналитики и отчетов

Типы направлений интеграции потоков данных:

•*Однонаправленные* — Данные передаются от конечных систем в централизованное хранение данных для дальнейшей обработки и анализа. Преимущества: простота построения решения, исходные данные доступны только для чтения. Подходит для анализа и построения отчетности. К недостаткам можно отнести отсутствие возможности по интеграции в бизнес процессы.

•*Двунаправленные (интерактивные)* – Данные передаются в обоих направлениях, как от конечных систем в централизованное хранение данных для дальнейшей обработки и анализа, так и обратно для интеграции в бизнес процессы (акцептование и т.п.). Преимущества: возможность интегрироваться в бизнес процессы. Обычно реализуется на уровне приложения. Недостатки: сложность построения решения, данные могут быть модифицированы внешними системами, что требует более высокого уровня информационной безопасности, сложности сопровождения.

Комплексная Интеграции Информационных Систем Предприятия

Принимая во внимание общую концепцию построения Системы Управления Бизнесом (Management Information System), вопросы интеграции различных Информационных Систем между собой является неизбежным «злом». Задача ИТ знать об этом и быть готовым снизить риски и негативное влияние на бизнес и ИТ Архитектуру Предприятия. При построении комплексной интеграции предприятия необходимо принять во внимание структуру организации. Модель интеграции Информационных Систем полностью зависит от структуры организации. Интеграция ИС Предприятия может происходить на различных уровнях:

Интеграция различных информационных систем *на организационном уровне*:

- в пределах одной компании
- в пределах портфеля
- в пределах холдинга

Интеграция различных информационных систем *на уровне бизнеса деятельности*:

- По функциям (департаментам),
- По процессам
- По сфере деятельности

Интеграция различных информационных систем *на технологическом уровне*:

- инфраструктуры,
- платформы
- приложений
- базы данных
- данных

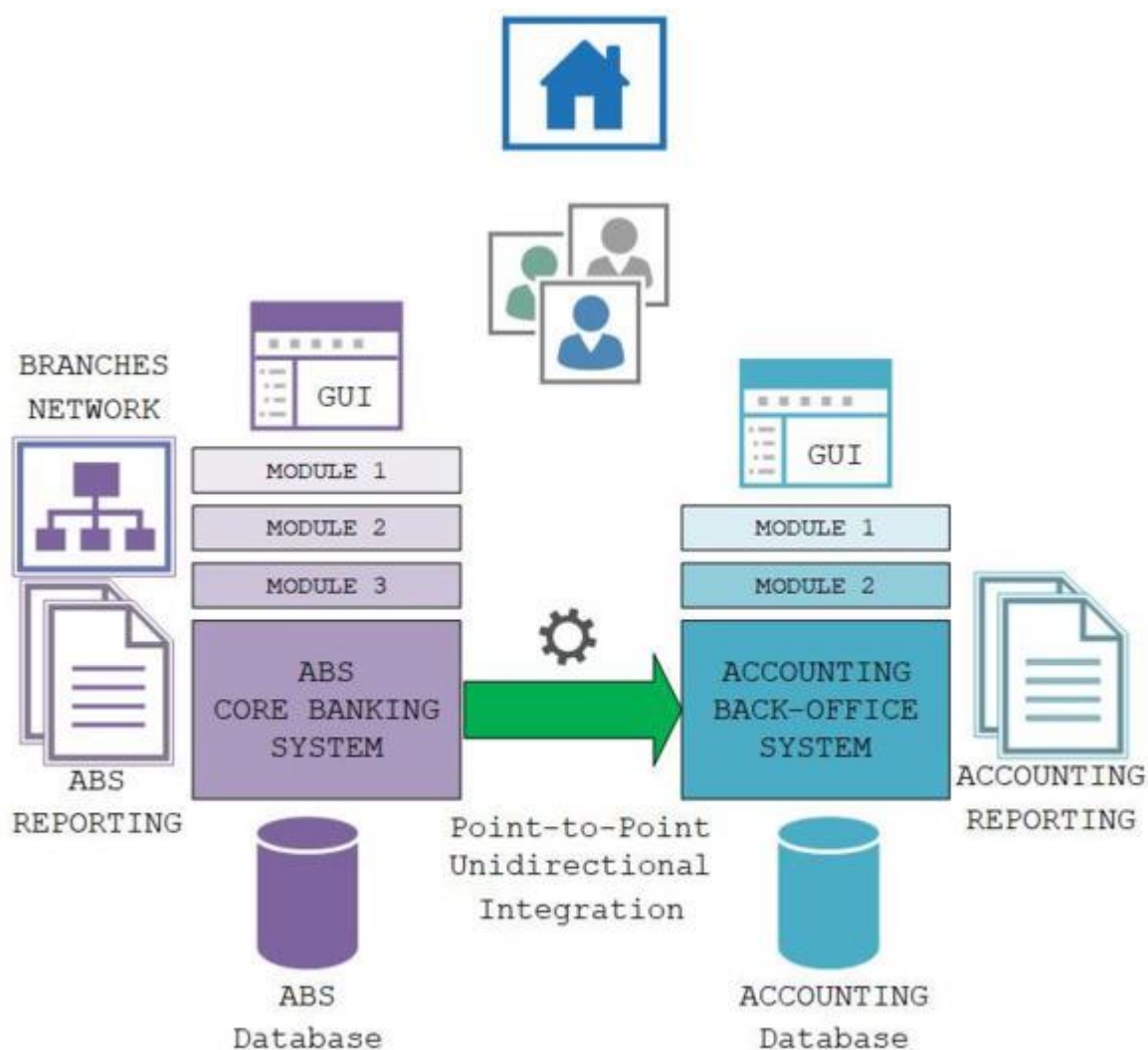
Степень Интеграция различных информационных систем:

- Частичная или Полная
- Ручная или автоматизированная
- Одно направленная или двух направленная

Рассмотрим более детально различные варианты интеграции с применением различных механизмов и типов.

Вариант 1: Интеграция двух информационных систем в масштабе одной компании

В качестве периферийной информационной системы выступает Автоматизированная Банковская Система (ABS), в качестве конечной системы программа ведения бухгалтерского учета (ACCOUNTING). Интеграции «одно направленного» типа с использованием механизма «Точка-точка» на уровне «Приложения» осуществляется от источника «ABS» к получателю «ACCOUNTING».



Все основные бизнес процессы происходят в АБС (создание клиентов, выдача кредита, все виды наличных оплат, в том числе и не банковского назначения, поступления переводов по погашению кредитов и т.п.). Транзакции из АБС выгружаются один раз при операции закрытия дня (Close of Business).

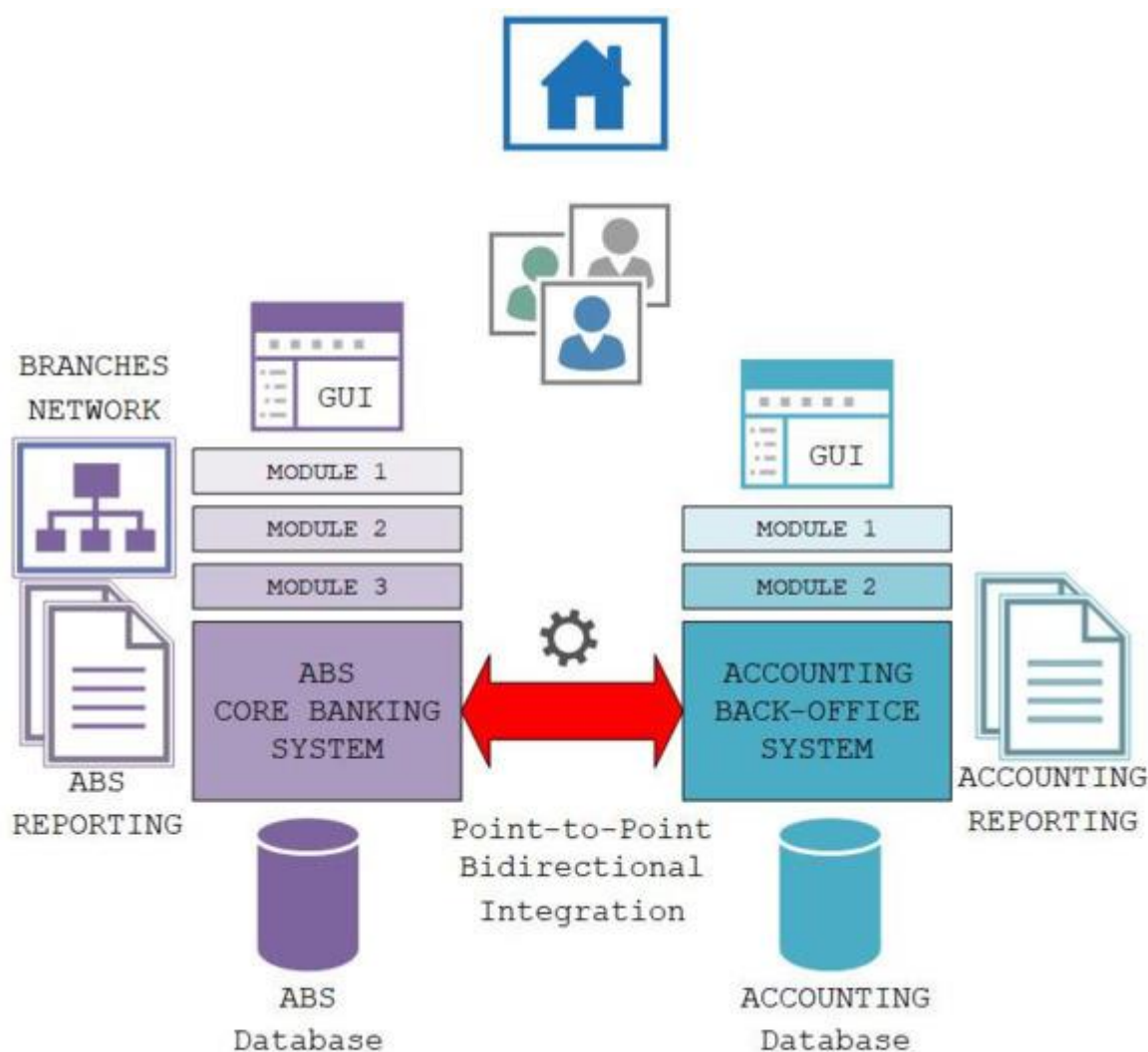
Бухгалтерская система обеспечивает ведение хозяйственных операций, бухгалтерского и налогового учета (амортизация, учет основных средств, безналичные переводы, не связанные с клиентами и т.п.).

Как пример пересекающихся процессов: новый поставщик вводится в АБС как потенциальный клиент, там же проводятся кассовые операции и т.п. Регистрация товара от поставщика производится в системе «Бухгалтерии» и т.п. Какие таблицы, поля, атрибуты должны быть переданы разбираются детально.

Подход к интеграции должен выполняться ТОЛЬКО С ПРИМЕНЕНИЕМ ПРОЦЕССНОГО ПОДХОДА!!!

Вариант 2: Интеграция двух информационных систем в масштабе одной компании

В качестве периферийной информационной системы выступает Автоматизированная Банковская Система (ABS), в качестве конечной системы программа ведения бухгалтерского учета (ACCOUNTING).



Вариант 2

Интеграции «двух направленного» типа с использованием механизма «Точка-точка» на уровне «Приложения» осуществляется между «ABS» и «ACCOUNTING».

Все основные бизнес процессы происходят в АБС (создание клиентов, выдача кредита, все виды наличных оплат, в том числе и не банковского назначения, поступления переводов по погашению кредитов и т.п.). Транзакции из АБС выгружаются один раз при операции закрытии дня (Close of Business).

Бухгалтерская система обеспечивает ведение хозяйственных операций, бухгалтерского и налогового учета (амортизация, учет основных средств, безналичные переводы), без ограничения.

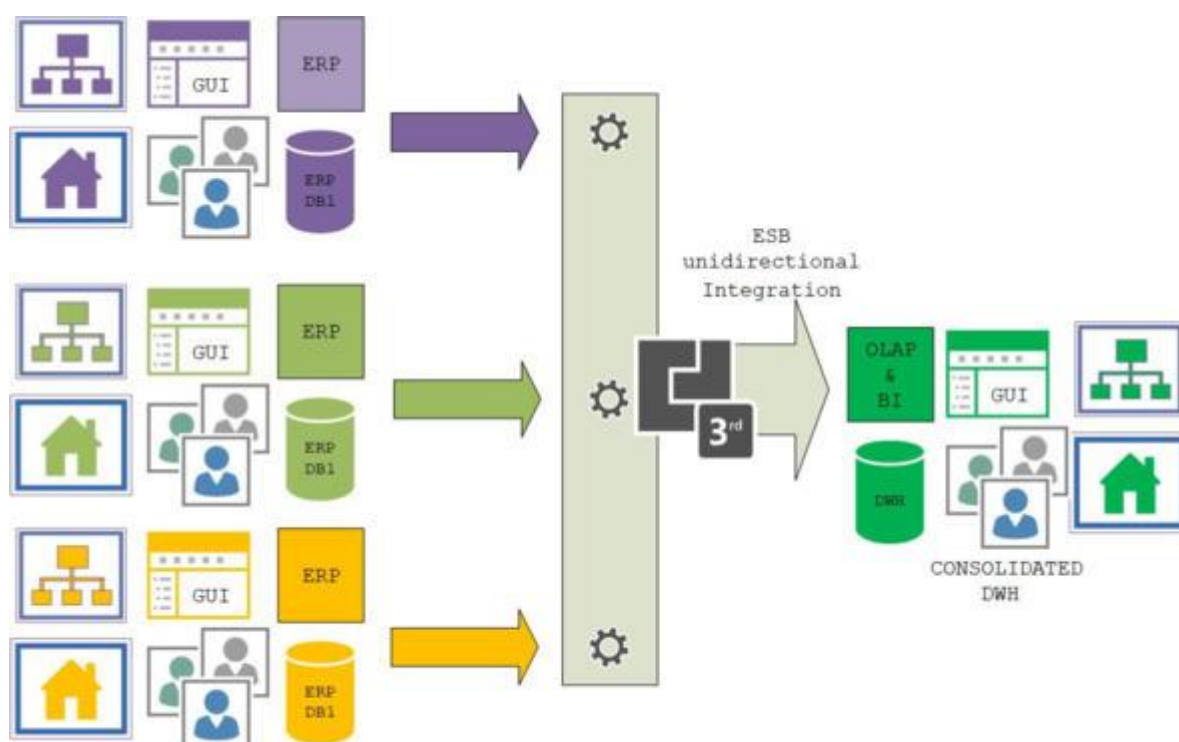
Как пример пересекающихся процессов: новый поставщик вводится в «Бухгалтерии», там же проводятся кассовые операции и т.п. Регистрация товара от поставщика производится там же и т.п. Данные по новому клиенту пересылаются в систему АБС.

В данном примере необходимо ввести дополнительные механизмы контроля (проверка внесенных изменений, исправления ошибок и т.п.). Более сложный вариант, но предоставляет большую свободу для департамента бухгалтерии. В приведенных примерах используется в качестве примера выделение бухгалтерского модуля. Относительная простота реализации так как основная деятельность банка связана с двумя сущностями: деньги и информация. Деньги выступают и в роли денег и товара.

Для производственных организаций ведение учета будет сложнее, так как имеются уже три сущности: деньги, товар (материал и произведенный товар) и информация. Кроме того, ситуация осложняется тем, что в процессе производства основные средства, рабочий труд передают часть стоимости для создается сущность «произведенный товар», вычислять себестоимость которого требуется рассчитать.

Вариант 3: Интеграция информационных систем различных компаний, объединённых в портфель или холдинг

Каждая компания имеет собственное ERP решение. Задача ИТ обеспечить сбор данных с различных систем в холдинг для последующего анализа и формирования отчетов для руководства. Для этого в холдинге развернута система OLAP & BI и система хранения данных (Data Warehouse DWH). Для обеспечения интеграции данных будет использоваться решение ESB «шина».



Требования по внедрению решения: наличие разработчиков на стороне компаний для обеспечения выгрузки данных, каналы связи для передачи данных и команда разработчиков на стороне холдинга. Команда разработчиков холдинга совместно с представителями бизнеса определяет данные, необходимые для передачи в холдинг, метод выгрузки, периодичность. На стороне компаний разрабатывает выгрузка данных в формате, поддерживаемым интеграционной «шиной». Настраивается интерфейс получения данных, их трансформации и передачи в дата центр. *Преимущества данного решения:*

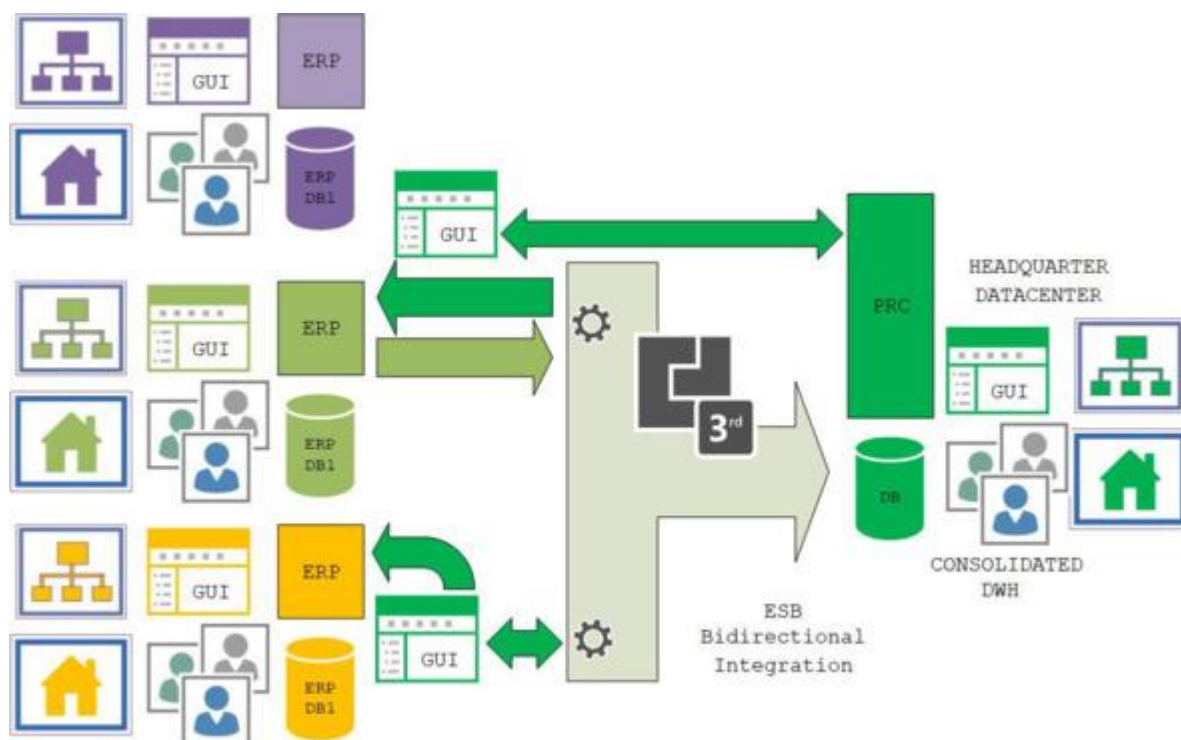
- относительная простота внедрения и сопровождения
- не высокая стоимость решения
- минимальные риски негативного воздействия на конечные системы и бизнес процессы в компаниях
- внедрение может проходить последовательно, и как следствие не потребует значительных человеческих ресурсов

К недостаткам решения можно отнести следующие:

- Система обладает только возможностями создания отчетов и аналитики.
- Точность и достоверность информации зависит от ввода данных на местах.
- Нет возможности интерактивного влияния на бизнес процессы в компаниях.

Вариант 4: Интеграция информационных систем различных компаний, объединённых в портфель или холдинг

Рассмотрим теперь интеграцию информационных систем различных компаний, объединённых в портфель или холдинг.



Вариант 4

Каждая компания имеет собственное ERP решение. В руководстве холдинга принято решение внедрить политику «Проведения тендера и закупок». Разработаны правила, определение лимиты по суммам и состав «ролевой» матрицы. Сотрудники холдинга должны непосредственно участвовать в процессе принятия решения. Технически политики реализованы с помощью информационной системы «PRC».

В первой компании (самая верхняя), текущая система управления не позволяет реализовать требования холдинга. В этом случае, компания использует решение «PRC» у себя в компании. Преимущества – единое решение, простота внедрения. К недостаткам можно отнести то, что данные в системе «PRC» не как не связаны с внутренней системой ERP компании.

Для нижней компании – имеется собственное ERP решение, которое имеет в своем наборе базовые функций, которые позволяют частично реализовать требования холдинга. Как вариант компания может использовать интерфейс программы «PRC». Интеграция, настраивается таким образом, чтобы была возможность обмена данными между системами.

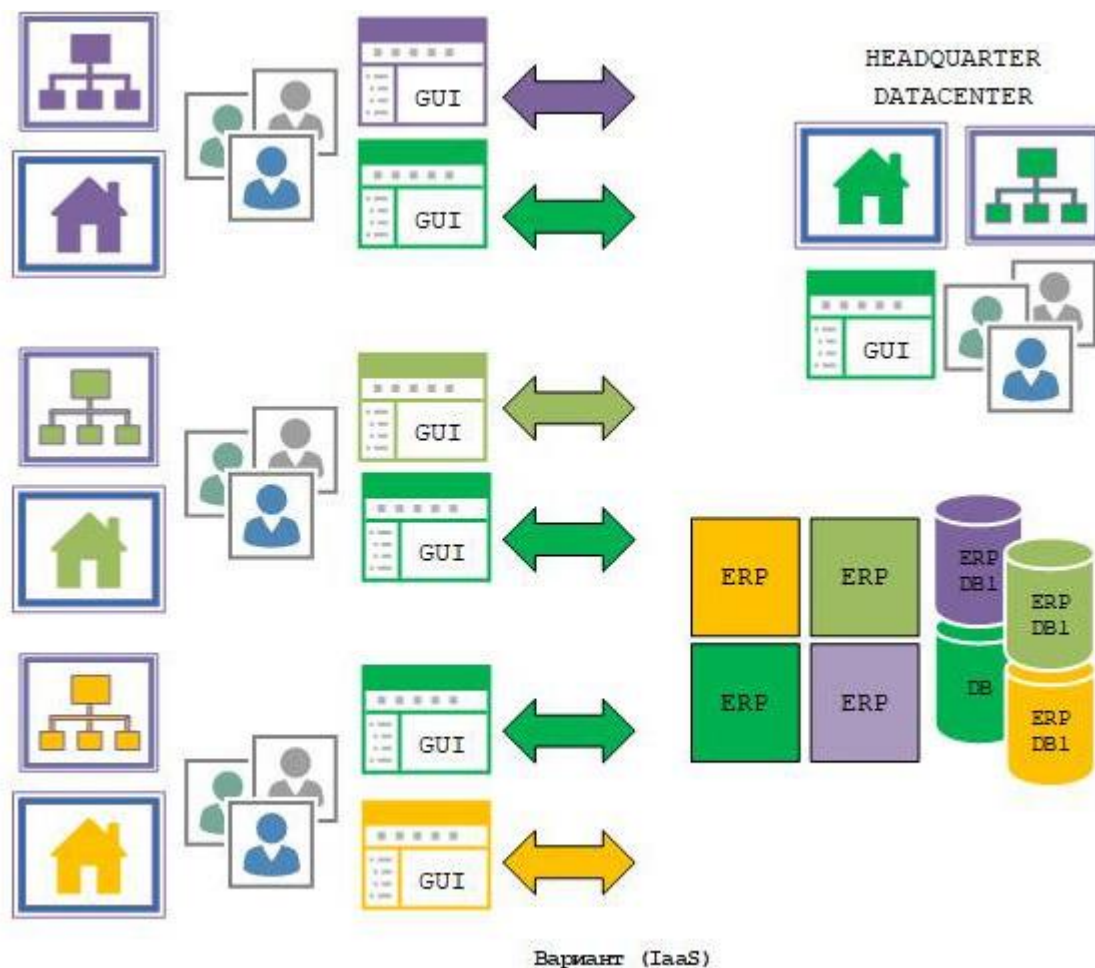
И третий случай – (компания, расположенная по середине). В компании имеется собственное решение ERP в которой имеется полный набор функций, требующих реализацию политики «Проведения тендера и закупок». Компания продолжает использование собственной программы, полностью интегрировав с решением «PRC».

Интеграции Информационных Систем Предприятия и централизация ИТ

Вопросы интеграции можно рассматривать в разрезе централизованного управления и предоставления ИТ сервисов. Далее на картинках представлены следующие три варианта предоставления сервисов и их интеграция в рамках холдинга:

Инфраструктура как Сервис (IaaS)

Холдинг предоставляет инфраструктуру дата центра для размещения ИТ систем компаний в нем. Каждая компания продолжает использование собственных информационных систем. Кроме этого ИТ холдинга предоставляет ИТ услуги и сервисы общего назначения. Преимущества данного решения – происходит консолидация вычислительных ресурсов в едином месте, снижение прямых и косвенных расходов на внедрение и сопровождение ИТ инфраструктуры, повышается уровень защиты ИТ активов.

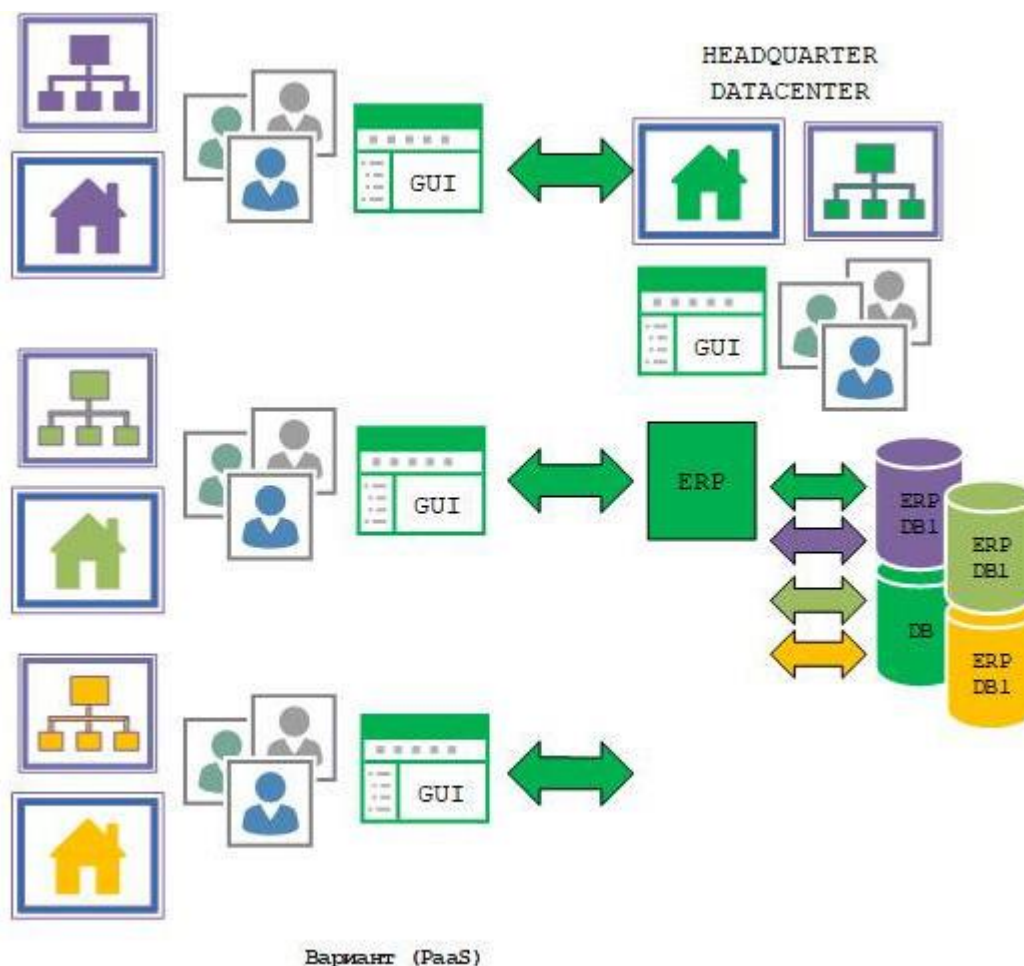


Процесс может происходить с минимальными рисками воздействия на информационные системы компаний. Данная модель подходит для начального этапа централизации ИТ или же для уровня холдинга, с различными направлениями деятельности, когда информационные системы кардинально различаются по своей функциональности (например, Автоматизированная Банковская Система АБС, система Управления Сельскохозяйственным Предприятием УСХП, Система управления отелями и ресторанами и т.п.). Результаты можно увидеть непосредственно после интеграции.

Платформа как Сервис (PaaS)

Холдинг предоставляет инфраструктуру дата центра для размещения ИТ систем компаний в нем. В качестве бизнес системы выбирается единая платформа приложения. Все предприятия используют единую платформу в рамках портфеля или группы компаний, объединённых схожей деятельностью (сельское хозяйство, производство, строительство и т.п.). При этом у каждой компании имеется собственная база данных и конфигурация. Преимущества данного решения – помимо всех преимуществ IaaS, данное решение позволяет упростить внедрение и сопровождение систем, благодаря тому, что имеется одна платформа приложения, что удобно как для ИТ персонала, так и для сотрудников организации (обучение одной системе). Возможность получения сводных отчетов (отчеты нескольких компаний портфеля). Вопрос интеграции данных упрощается за счет унификации платформы. При этом каждая компания сохраняет свою идентичность и автономность, так как конфигурация и данные каждой компании хранятся в собственной базе. Данная модель подходит для второго этапа централизации ИТ или же для уровня портфеля, группы компаний, имеющие схожие направления деятельности, или же внедряются общие функции для всех компаний холдинга или группы компаний. Для

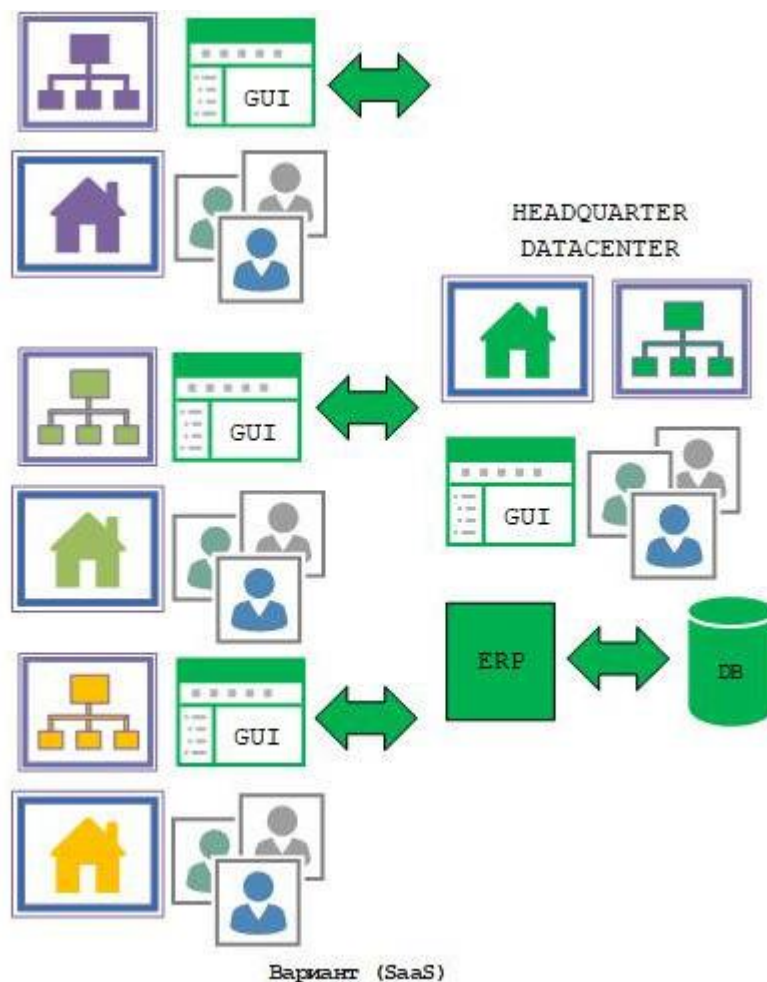
выполнения данного этапа крайне важно ответить на два вопроса: первый – в чем цель и конечный результат, и второй – иметь четкую диаграмму всех бизнес процессов организации в целом, и компаний в частности. Для реализации данного плана, необходима заинтересованность руководства холдинга, поддержка руководства на местах, и тесная интеграция специалистов бизнеса и ИТ, хорошо разбирающихся в деталях процессов, происходящих в компании. Переход на унифицированную платформу, может потребовать дополнительные финансовые инвестиции, возможно значительные, и временные рамки, как для анализа, так и для поэтапного внедрения. Не стоит ожидать быстрые результаты и победы.



Результаты интеграции будут видны только в долгосрочной перспективе. С точки зрения бизнеса остаются такие недостатки как: не унифицированная информация по справочникам и номенклатуре продуктов, план счетов и т.п. Проблемы будут усугубляться по мере детализации данных с различных компаний на уровне портфеля.

Программа как Сервис (SaaS)

Холдинг предоставляет инфраструктуру дата центра для размещения ИТ систем компаний в нем. В качестве бизнес системы выбирается единая платформа приложения и база данных. Все предприятия используют единую платформу в рамках портфеля или группы компаний, объединённых схожей деятельностью (сельское хозяйство, производство, строительство и т.п.).



Данные каждой компании хранятся в единой информационной системе холдинга. Преимущества данного решения – помимо всех преимуществ IaaS и PaaS предоставляет единую информационную систему холдинга. Каждая компания является частью холдинга. Информация по справочникам, номенклатуре, плану счетов унифицирована имеется возможность формирования консолидированных (суммированных по статьям) отчетов. Возможность интерактивного воздействия в процесс управления (авторизация и т.п.) со стороны руководства портфеля или холдинга. Данная модель подходит для финального этапа централизации ИТ. Как и для предыдущей модели, крайне важно ответить на два вопроса: первый – в чем цель и конечный результат, и второй – иметь четкую диаграмму всех бизнес процессов организации в целом, и компаний в частности. Для реализации данного плана, необходима заинтересованность руководства холдинга, поддержка руководства на местах, и тесная интеграция специалистов бизнеса и ИТ, хорошо разбирающихся в деталях процессов, происходящих в компании. Переход на унифицированную платформу, может потребовать значительные финансовые инвестиции и временные рамки, как для анализа, так и для поэтапного внедрения. Результаты интеграции будут видны только в долгосрочной перспективе. Данный этап характерен высоким риском в процессе интеграции. Кроме этого, процесс вывода компании из состава организации или холдинга может быть так же достаточно сложным и болезненным. Процесс доработки функционала для каждой компании, общий для всех компаний.

Проблемы выбора ИТ-решения для Бизнеса

Информационные Системы бизнеса находятся на стыке взаимодействия бизнеса и ИТ. В этом кроется основная сложность, и является источником возникновения конфликтов, недопонимания и недовольства. Остро встают вопросы и проблемы, освещенные в данной книге ранее, в главе «Концепция построения Архитектуры Предприятия». При этом не имеет значения масштаб

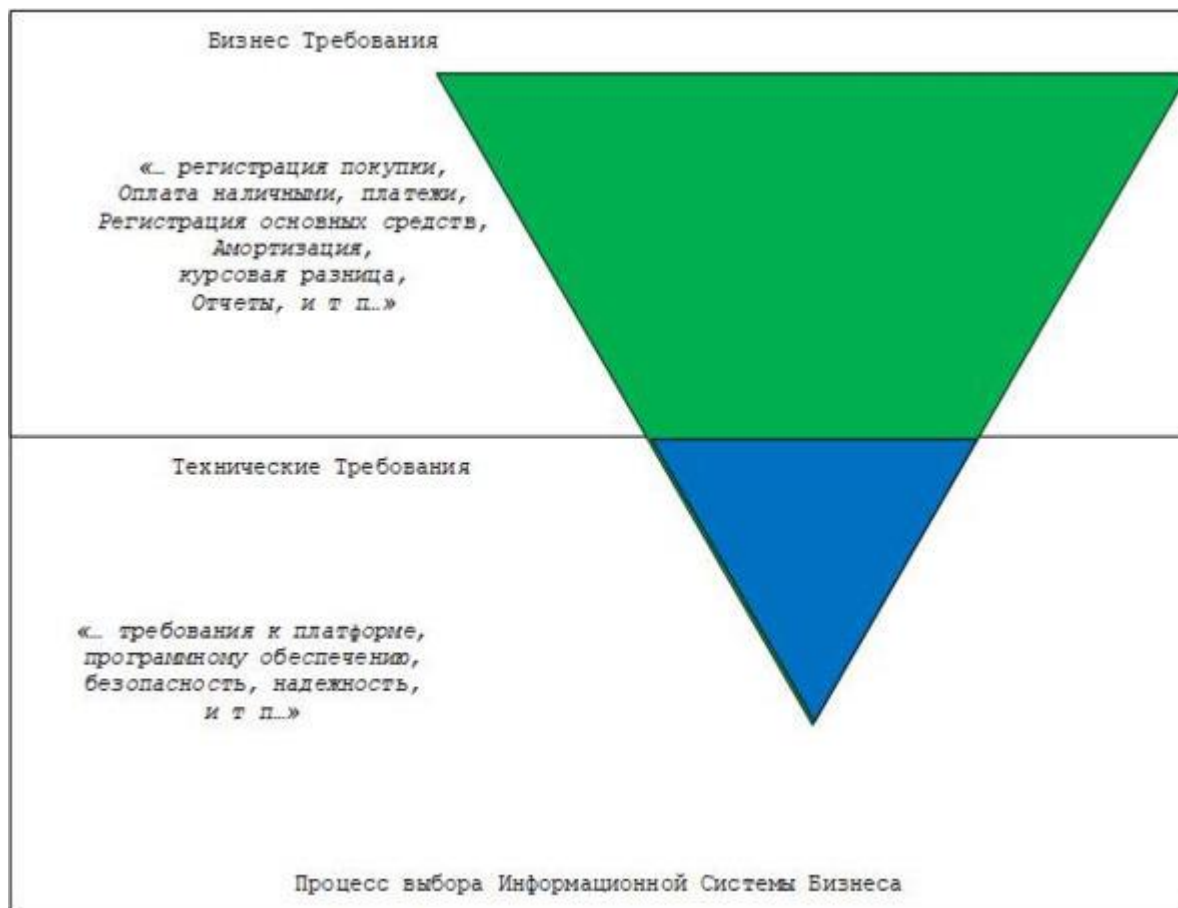
организации (небольшая автономная компания или сложный холдинг со множеством направлений бизнеса), фаза становления (начало ведения бизнеса или долгое и устойчивое пребывания на рынке) или уровень компетенции сотрудников (молодой специалист, только закончивший институт или «матерый» сотрудник с огромным стажем по своей специальности) проблемы у всех одни и те же вопрос только насколько у кого «болит».



Так при выборе Информационной Системы сугубо технического направления (защита периметра, системы Антивирусной защиты и т.п.) или общего назначения (Сервис предоставления файлов в совместное использование, системы почтовых сообщений и т.п.), выбор решения фактически полностью зависит от технических специалистов в области ИТ или Информационной Безопасности. Они говорят на одном «языке»; разбираются в особенностях решений, требованиям предъявляемых к системам и т.п. Взаимодействие с бизнесом минимальное. Бизнес требования со стороны бизнеса могут быть сформулированы одним предложением: «... чтобы можно было посылать и принимать почту...». Как видно из рисунка, «вершина айсберга» – бизнес требования видны сотрудникам организации лишь часть общих требований к системе.

Вся суть коммуникации между бизнесом и ИТ сводится на пример к запросу, как слышит бизнес: «... дайте деньги на память...», что на языке ИТ сотрудников значит: «... Выделите финансирование на закупку модулей оперативной памяти для серверов...».

При выборе Информационной Системы для бизнеса, со стороны ИТ требования к системе остаются фактически таким же, как и прежде, но «айсберг» переворачивается и центр смещается к требованиям бизнеса. Хорошо, если бизнес может сформулировать требования, как в общем, так и с учетом специфики конкретной организации, что позволит ИТ разработать или купить решение, удовлетворяющее требованиям бизнеса и вписывающиеся в общую ИТ Архитектуру. На практике, часто руководство бизнеса самостоятельно принимает решение без обсуждения с представителями ИТ, что в конечном этапе приводит к «зоопарку» решений, не эффективному использованию систем и высокой стоимости сопровождения. Или же требования бизнеса сформулированы очень обширно «... нужна система для ведения бухгалтерского учета...», а вы ИТ должны найти и выбрать.



Даже если представители бизнеса прекрасно понимают, что им нужно, умеют правильно сформулировать свои требования, ясно видят перспективы роста бизнеса и прочие нюансы, важные в процессе выбора решения – это всего лишь решает внутреннюю проблему. Необходимо обратить внимание на внешнюю сторону проблемы.

Ситуация выбора ИТ-решения усугубляется тем фактором, что на современном рынке помимо достаточно широкого выбора самих систем появились различные варианты приобретения и внедрения этих систем. Одну и ту же систему можно заказать «под ключ» у компании производителя или же приобрести у производителя и самостоятельно внедрить силами сотрудников ИТ подразделения предприятия) или силами интегратора.

Следующим фактором, который влияет на выбор ИС, а также способа ее приобретения, являются критерии, по которым принимается решение в пользу той или иной системы. В большинстве случаев при выборе ИС ИТ-директора руководствуются экономическими эффектами, однако даже в этом случае ситуация является непростой. Так, помимо затрат на реализацию проекта по внедрению, необходимо учитывать затраты на совокупное владение системой, которые включают затраты на поддержку и развитие системы, обучение персонала, обновление оборудования, косвенные затраты (простои, отказы ИС и др.) и риски. При этом статистика говорит о том, что при сроке эксплуатации ИС в 3 года стоимость владения системой сравнивается (а очень часто и превышает) с затратами на внедрение ИС. Помимо экономических показателей, критериями при выборе ИС могут являться дополнительные факторы: скорость введения системы в эксплуатацию, наличие дополнительной функциональности в платформе, риски при реализации проекта и др. Таким образом, даже с учетом только экономических факторов, задача выбора ИС является многокритериальной. Наличие нескольких критериев усугубляется тем, что необходимо определить приоритеты или предпочтения каждого из критериев, чтобы решение о выборе ИС максимально соответствовало предпочтениям ИТ-директора и стратегическим целям предприятия.

Нельзя также не учитывать тот факт, что и оценка эффективности, и рассмотрение критериев производятся не одним человеком. Зачастую решение о выборе информационной системы

формируется у ИТ-руководителя на основании мнений одного, а чаще нескольких экспертов. При этом каждый эксперт имеет свою точку зрения на проблему, которая чаще всего отличается от видения этой же проблемы другим экспертом. Мнения могут отличаться как в оценках эффекта от внедрения ИС (затраты и положительные эффекты), так и приоритетности критериев. Таким образом, многокритериальную задачу выбора ИС приходится решать на основании экспертных мнений нескольких лиц, что еще более усложняет выбор ИС.

С другой стороны, выбор бизнес решений производится зачастую узким кругом руководителей без привлечения ИТ, что часто приводит к выбору по принципу: «... давайте возьмём как у той компании, если у них работает, то и у нас тоже будет...», или «... давайте возьмём самое дорогое решение – оно, наверное, самое лучшее...», или что еще хуже преследуя какие-то свои скрытые цели.

Рекомендации по выбору Информационной Системы Управления

Ни одна из методик оценки эффективности Информационной Системы, ни совместное использование нескольких методик не позволяет однозначно решить задачу выбора той или иной информационной системы. Сейчас на рынке представлено огромное множество решений, реализующих одни и те же бизнес-функции. Как правило, ИТ-проект на предприятии является комплексным и предполагает реализацию нескольких направлений и бизнес-функций. Предлагаемые ИТ-решения также обладают достаточной гибкостью благодаря модульной архитектуре. В результате ИТ-директор сталкивается с необходимостью решить задачу, какие бизнес-функции ему необходимо реализовать сейчас, какие заложить на реализацию в будущем, а от каких необходимо и вовсе отказаться. То есть важно расставить приоритеты в функциональности ИС и запланировать ее развитие в будущем. В таком случае мы получаем целый набор вариантов ИТ-решений, из которого необходимо выбрать наиболее оптимальный как с точки зрения текущей функциональности, так и с точки зрения стратегического развития ИТ-комплекса предприятия в целом и оптимальности финансовых затрат.

Критерии выбора ИТ решения

В качестве основных критериев выбора решения, можно определить следующие:

- **Какие цели?**
- **Какие процессы необходимо контролировать?**
- **Размер организации:** (Small Business, Medium Business, Large Business)
- **Заявленные возможности продукта или решения.**
- **Удовлетворяют ли заявленные возможности требованиям бизнеса?**
- **Техническая Архитектура:**
 - *Архитектура решения:* (client-server, Client-Application Server-Database Server)
 - *Серверная платформа:* (Cloud based, Windows, Linux, Others)
 - *Варианты установки:* (Cloud based или On-premises)
 - *Поддержка виртуализации:* (Physical only, Hyper-V, VMware, Others)
 - *Поддерживаемые базы данных:* (Microsoft SQL, MySQL, Internal DB)
- **На стороне клиента:**
 - *Поддерживаемые устройства на клиенте:* (Windows, Linux, Android, Mac OS, iPhone/iPad, Web-based)
 - *Поддерживаемые языки интерфейса:* (Single English, Multi-Languages, Customer)
- **Архитектура отказоустойчивости и доступности**
- **Архитектура восстановления и архивирования**
- **Возможности масштабирования решения**
- **Как данное решение вписывается в общую ИТ архитектуру.**
- **«Купить или сделать?»** В зависимости от способа приобретения ИС показатели эффективности, в первую очередь финансовые, будут отличаться. К тому же каждый раз набор вариантов дополняет самостоятельная разработка ИС, которую также необходимо оценивать.
- **Оценка производителей и поставщиков решений** (Рейтинг, Наличие локального партнера (продажа / поддержка)
- **Модель внедрения:**

°*Стоимость*: (Free (Open-Source), One-time payment, Monthly payment, Annual subscription, Perpetual)

°*Лицензирование*: (Per servers, Per hosts, Per operators/agents, Per modules, Per users, Per CPU/core, Per modules)

°*Варианты подписки и версий*

•**Модель сопровождения**: (Technical support, Update support)

°*Стоимость*: (Free, Annual fee, Basic Technical support, Local support, Remote support)

°*Лицензирование*

°*Возможности по обновлению продукта*: (Update patches, Upgrade packs, Re-installation)

•**Возможности интеграции**: с имеющимися решениями, с потенциально возможными решениями

В качестве общих рекомендаций по выбору ИТ решения для бизнеса я бы рекомендовал следующие варианты выбора в зависимости от имеющихся условий. Если бизнес не имеет четкого представления, какие требования предъявляются к системе, высокий уровень неопределённости в следствии объективных (направление деятельности новое для бизнеса, условия рынка и т п) или субъективных причин (низкий профессиональный уровень сотрудников, слабая или не определённая административная организация и т п), то возможны следующие варианты:

•Организация покупает недорогое, быстро внедряемое решение с набором базового функционала, для использования в течении года или двух. Цель – сформировать рабочие бизнес процессы, обучение персонала.

•Организация пытается разработать решение собственными силами. При том ИТ внедряет новый функционал по требованию со стороны бизнеса. Данный подход может занять больше времени для достижения тех же целей, что и в предыдущем варианте, но имеет ряд своих преимуществ, а именно – бизнес и ИТ получают более глубокое понимание бизнес процессов, система относительно проста так как имеет в своем наборе только необходимый функционал. Дальнейшее развитие может происходить по двум направлениям – система дорабатывается и становится основным решением для организации, или же на базе решения формируется «техническое задание» для выбора решения уровня предприятия.

•Организация выбирает имеющееся на рынке готовое решение с расширенным набором функций. Данное решение является основным для бизнеса и на его базе сотрудники постепенно осваивают бизнес процессы.

Этапы выбора ИТ решения

Можно определить следующий порядок действий по ИТ проекту.

На первом этапе:

- Сбор требований со стороны бизнеса – инициатора проекта (бизнес требования)
- Добавление технических требований со стороны департамента Безопасности
- Добавление технических требований со стороны ИТ департамента

На втором этапе:

- Поиск решений, без ограничений по стоимости, архитектуре и т п.
- Сбор заявленных возможностей решения

На третьем этапе:

- Анализ решений (со стороны бизнеса) на соответствие бизнес требованиям
- Анализ решений (со стороны ИТ департамента) на соответствие требованиям, архитектуре и т п

•Формирование «короткого» списка решений удовлетворяющих всем требованиям. При необходимости проводится обращение к департаменту Снабжения для получения предложений

На четвертом этапе:

- Детальный анализ решения, выбор архитектуры, производителя, определение бюджета и т п
- Принятие решения по бюджету, срокам (со стороны бизнеса)
- Формирование технического задания для проведения тендера
- Формирование плана внедрения (частичное, полное и т п)
- Выбор «короткого» списка победителей

- Уточнение последних изменений и дополнений
- Финальный тендер (по необходимости) для «короткого» списка компаний

На пятом этапе:

- Закупка
- Подготовка к внедрению
- Внедрение
- Корректировка
- Сопровождение
- Обновление и улучшение
- Вывод из эксплуатации

Метод Покупки Готового Решение (COST или «OFF-the-SHELF»)

COST или («OFF-the-SHELF» коробочное готовое решение) – Одним из подходов является покупка готовых решений. При покупке такого программного обеспечения организация должна:

- понимать достоинства и недостатки этого подхода;
- формализовать процесс выбора наиболее эффективного готового решения;
- определить процесс для эффективной интеграции и настройки готового решения;
- определить функциональные требования на приемлемом уровне;
- сформировать перечень управленческих и операционных требований;
- определить требования к продукту и поставщику;
- определить требования к интеграции услуги.

При покупке решения остается необходимость в:

- кастомизации (customization) – адаптация продукта под требования клиента, первоначальное конфигурирование, настройка интерфейса, изменение бизнес процессов и т п,
- локализация (localization) – язык интерфейса, перевод печатных форм и т п.

Основные преимущества – Покупка готовых пакетов программного обеспечения более экономична, часто более быстрое решение при выборе и внедрении. Может быть представленная клиенту как действующая «модель» или «прототип». Клиент уже на этапе выбора решения может иметь полную картинку возможностей и внешнего вида конечного продукта, имеющиеся ограничения и т п.

К недостаткам можно отнести – менее гибка, чем разработка собственных решений.

Концепция Информационной Безопасности

Общие Положения

Данный раздел содержит основные принципы архитектуры и информационной безопасности которые должны быть приняты во внимание. Раздел основывается на международных стандартах и практиках в области информационной безопасности, таких как серия ISO/IEC27000, ISO/IEC27001, ISO22301:2012, ISO15408, ISO17799 (BS7799), NIST серии 800-xx, Information Security Forum (ISF).

DEFENSE IN DEPTH LAYERS

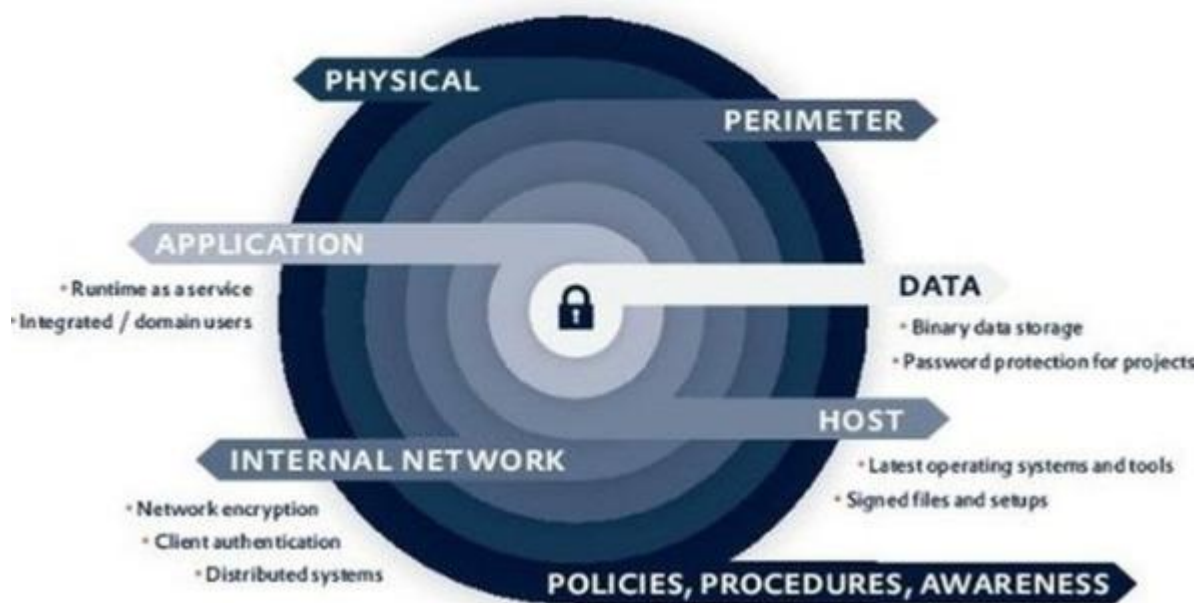


Диаграмма Концепция «Defense in Depth»

Задачи Информационной Безопасности

Обеспечение информационной безопасности способствует решению следующих задач:

- определение целей обеспечения информационной безопасности компьютерных систем;
- создание эффективной системы управления информационной безопасностью;
- расчет совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям;
- применение инструментария обеспечения информационной безопасности и оценки ее текущего состояния;
- использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения разработчиков информационных систем, позволяющих объективно оценить защищенность информационных активов и управлять информационной безопасностью компании.

Необходимо определить приоритеты по критериям (Confidentiality, Integrity and Availability CIA):

- Конфиденциальность (Confidentiality)
- Целостность (Integrity)
- Доступность (Availability)

Данные приоритеты требуется определить, как для организации в целом, так и для каждой ИТ системы.

Классификация информации и ИТ активов

Все ИТ активы и информация должны быть классифицированы с точки зрения безопасности по уровню конфиденциальности. Обязательные требования для обеспечения конфиденциальности:

- Классификация данных.
- Наличие политики определяющей уровни доступа.
- Наличие процедур по работе с данными каждого класса.

Классификации данных может быть построена на основе следующих условий:

- Требования устанавливаются регулируемыми органами.
- Требования определяются внутри компании.
- Классификация данных установленных регулируемыми органами не может быть понижена
- Доступ к данным предоставляется по принципу «минимальных привилегий»

Классификация данных по уровню доступа:

Общего доступа – Могут быть опубликованы за пределами компании (например, перечень товаров и услуг, цены и т.п.)

Внутреннего использования – Документы предназначенные для сотрудников компании. Утечка данных за пределы компании не наносит ущерба компании (процедуры, принятые в компании и т.п.)

Конфиденциальные – Данные содержат информацию, разглашение которой может нанести ущерб компании (репутации, финансовые потери и т.п.). Контроль за данными не регламентируется внешними контролирующими органами, но являются важными с точки зрения руководства компании (пароли к системам, контактные данные руководителей и т.п.).

Секретные – Данные регламентируются внешними контролирующими органами и разглашение которой наносит ущерб компании (репутации, финансовые потери и т.п.). к ним можно отнести финансовые данные клиентов и т.п.

Классификацию данных необходимо проводить с представителями бизнеса и функциональных департаментов компании. Для определения информационных потоков и уровня интеграции данных необходимо провести классификацию данных информации по ряду атрибутов:

Зона покрытия – Данные локального значения и представляющие ценность для одной компании. Как пример; заказ столиков, обслуживание официантом в разрезе столиков/клиентов. Данная информация может быть интересна для одной компании (отеля) и не представляют ценность для других компаний компании, наиболее востребованные комнаты, меню и т.п. может быть интересна для портфеля и т.п.

Зона видимости – Кому предназначены данные. Например, финансовые данные портфелей и компаний могут видеть только представители финансового департамента компании и правление, но представитель портфелей не видит информацию другого портфеля.

Тип данных – Бизнес информация или же техническая.

Владелец данных – подразделение или лицо, отвечающее за работу с информацией (целостность и доступность). Необходимое контактное лицо для получения дополнительной информации и данных по процессу и т.п.

Классификация данных по ИБ – (коммерческая тайна, внутреннего пользования и т.п.). Данные по клиентам, которые могут быть переданы компаниям компании или нет. (контактные данные клиентов отелей могут быть интегрированы в единую систему управления клиентами (CRM) и в дальнейшем использоваться в маркетинговых целях для поиска потенциальных клиентов и т.п.)

Происхождение данных – Данные являются первичными, извлечены из бизнеса системы или же являются производными после проведения аналитических вычислений. Как пример имена, и контактная информация клиентов (Hospitality) может рассматриваться как первичные данные, а список потенциальных клиентов для Retail Group проанализированный в системе (Hospitality) по ряду показателей (платежеспособность, количество потраченных средств, поведения клиента и т.п.) может рассматриваться как производные данные.

Источник данных – Веденный вручную оператором и наименование системы.

Уровень достоверности данных – данные внесены из установленных источников или являются предположениями и умозаключениями.

Для контроля информации можно ввести *«Маркер безопасности»* – буквенно-цифровой идентификатор, определяющий уровень конфиденциальности документа.

Определение потоков данных

Потоки данных должны быть описаны для каждой категории информации с указанием дополнительных атрибутов.

Идентификация пользователя

Все пользователи ИТ сервисов уникально идентифицированы в системах (учетная запись пользователя домена, почтовой системы, пользователь бизнес приложения и т.п.). Доступы к ИТ активам должны предоставляться на уровне групп. При проведении расследований инцидентов или нарушения информационной безопасности опираются на учетную запись пользователя. Все действия, связанные со сменой прав доступа или атрибутов учетной записи (пароля и т.п.) должны фиксироваться. Пользователь несет ответственность за любые действия, связанные с активностью его учетной записи.

Классификация по группам доступа и ролям

Все пользователи ИТ сервисов должны быть сгруппированы по группам и ролям. Доступы к информационным системам и сервисам предоставляются на уровне групп. Доступы сотрудников ИТ департамента также должны быть разграничены по группам, в зависимости от выполняемых действий и привилегий. Процесс предоставления прав доступа и членства в группах должен быть соответственно организован и документирован.

Принцип Минимальных Привилегий

При предоставлении права и доступов всем пользователям ИТ систем и сотрудникам ИТ необходимо руководствоваться правилами «минимальных привилегий».

Использование лицензионного программного обеспечения

Использование лицензионных программных продуктов в «рабочей» среде является обязательным требованием для всех без исключения функций и подразделений организации.

Организация процесса Информационной Безопасности

Ключевые компоненты

В процессе управления Информационной Безопасности учитываются следующие ключевые показатели и определения:

- Должны участвовать как минимум Бизнес департаменты компании, департамент Внутренний Аудит, департамент Безопасности, Финансовый департамент, департамент Управления Рисками, департамент Отдел Кадров и ИТ департамент или подразделения исполняющие их функции.
- Организационная структура компании должна должным образом управлять «конфликтом интересов» департаментов

•Бизнес департаменты определяют классификацию информации в соответствии с бизнес процессами

•Департамент Рисков проводит оценку рисков

•Департамент Безопасности предоставляет рекомендации по вопросам Информационной Безопасности

•Департамент Управления Кадрами обеспечить обучение и ознакомление работников с информацией касательно Информационной Безопасности

•Департамент Внутреннего Аудита проводит анализ на соответствие нормам и процедурам, а также необходимый мониторинг

•Департамент Безопасности обеспечивает физическую защиту ИТ активов

•Департамент Безопасности ведет мониторинг активности, связанной с ИБ

•ИТ департамент обеспечивает защиту и управление ИТ активами

•ИТ департамент разрабатывает необходимую документацию

Разделения Обязанностей в рамках организации

Различают различные принципы и подходы к разделению обязанностей между департаментом Безопасности и ИТ, например, департамент Безопасности выполняет непосредственное управление, внедрение и сопровождение сервисов информационной безопасности ИТ инфраструктуры. Можно выделить следующие модели разделения обязанностей:

•*Департамент Безопасности непосредственно управляет системами информационной безопасности.* К ним может относиться системы защиты периметра, предоставления доступа в интернет, защиты почты и т.п. ИТ департамент непосредственно управляет ИТ системами.

•*Департамент Безопасности непосредственно управляет частью функций в системах, связанных с информационной безопасностью.* К ним можно отнести настройка правил и политик на фаервола, активация и деактивация пользователей и т.п. ИТ департамент непосредственно управляет ИТ системами и системами ИБ.

•*Департамент Безопасности и департамент ИТ совместно непосредственно управляют системами информационной безопасностью и ключевыми ИТ сервисами.* Реализация возможна как административными действиями: одна учетная запись – две части пароля у разных департаментов, или же с помощью специализированных средств.

Для большинства организаций может подойти следующий подход:

•*Департамент Безопасности – является «владельцем» ИБ.* Обеспечивает физическую безопасность ИТ активов, определяет требования к системам безопасности в целом и информационной безопасности, политики ИБ и т.п. Выполняет контрольные функции в отношении надлежащего и своевременного исполнения ИТ департаментом требований ИБ. Непосредственно управляет такими системами безопасности, как система контроля доступа (физическая), система видеонаблюдения, системы оповещения о пожаре и проникновении. По отношению к ИТ департаменту в вопросах безопасности является «головой».

ИТ департамент – в рамках информационной безопасности, является «управляющим» информационных систем, комплекса информационной безопасности. Сотрудники ИТ департамента выполняют непосредственное конфигурирование, внедрение и сопровождение компонентов инфраструктуры информационной безопасности. Предоставляют доступ «только для чтения» для сотрудников подразделения ИБ и передачу логов активности компонентов ИТ инфраструктуры. Оказывают техническое содействие департаменту безопасности по внедрению и сопровождению систем безопасности. В зависимости от количества и сложности решений, в составе ИТ департамента может существовать подразделение ИТ Безопасности, отвечающее за сервисы обеспечивающие информационную безопасность. По отношению к департаменту Безопасности является «руками».

Департамент Внутреннего Аудита – в составе комитета, формирует требования по организации взаимодействия департаментов, проводит контроль соответствия деятельности департаментов безопасности и ИТ требованиям руководящих документов. По отношению к департаментам Безопасности и ИТ по вопросам информационной безопасности является «глазами».

Преимущества данного подхода:

- Нет необходимости держать значительный штат в департаменте Безопасности, который по сути дублирует действия ИТ. При внедрении и сопровождении любого ИТ сервиса или информационной системы, вопрос по обеспечению информационной безопасности – обязательный.

- Простота разграничения прав и ответственности. «Безопасность» говорит, «ИТ» выполняет, «Безопасность» контролирует исполнение. Особенности большинства Информационных систем – ролевой доступ и наличие «Административного» доступа с максимальными привилегиями. Наличие двух администраторов в одной системе может приводить к конфликтам интересов, разбирательствам таким как кто-то что-то изменил, в логах не отражается и т.п.

- Наличие цепочки контролей и взаимный мониторинг. ИТ имеет максимальные возможности к информационным системам. За обладателями таких возможностей необходим надлежащий контроль. Фактически эта роль возлагается на департамент Безопасности, по принципу «Вы следите за всеми – мы следим за вами». Все действия ИТ отслеживаются и передаются за пределы ИТ департамента. В тоже время, ИТ отслеживает действия департамента Безопасности в рамках «обычных пользователей» систем.

Каждая модель имеет свои преимущества и недостатки. Выбор модели зависит от требований бизнеса, возможностей систем, политики компании и ее возможностей.

Модели Информационной Безопасности и защиты данных

Для обеспечения Информационной Безопасности в целом, и ИТ безопасности в частности применяются различные модели защиты конфиденциальности, целостности и доступности. Обычно применяются смешанные модели Информационной Безопасности.

В качестве основных моделей можно выделить следующие:

Bell La Padula – модель защиты конфиденциальности

Bell La Padula – модель (многоуровневой) защиты конфиденциальности. Построенная на модели «информационных потоков». Модель конечных автоматов, которая реализует аспекты защиты конфиденциальности на основе матрицы «Субъект-объект» с применением трех основных правил:

Simple Security Rule: Субъект НЕ МОЖЕТ ЧИТАТЬ данные на более высоком уровне.

Star Property Rule: Субъект НЕ МОЖЕТ ЗАПИСАТЬ данные на более низком уровне.

Strong Property Rule: Субъект МОЖЕТ ЧИТАТЬ и ЗАПИСАТЬ данные только на своем уровне.

Biba – модель защиты целостности

Biba – модель защиты целостности. Построенная на модели «информационных потоков». Модель использует сетку целостности. Основные принципы модели:

Integrity Axiom: Субъект НЕ МОЖЕТ ЗАПИСЫВАТЬ на верх

Simple Integrity Axiom: Субъект НЕ МОЖЕТ ЧИТАТЬ данные находящиеся на нижнем уровне

Invocation property: Субъект НЕ МОЖЕТ ЗАПРАШИВАТЬ обслуживание (call) у другого субъекта, находящегося на более высоком уровне.

State Machine Model

State Machine Model – модель защиты безопасности, основанной на состояниях (state).

Information Flow Model – модель защиты данных

Clark Wilson – модель защиты целостностью

Clark Wilson – модель защиты целостностью. Выполняет три основные цели:

- Предотвращает изменения не авторизованного пользователя
- Предотвращает выполнение не корректных изменений
- Обеспечивает согласованность «правильные транзакции»

Вводит понятия:

«Пользователь», «Transformation Procedure TP», «Constrained Data Item CDI», UDI, IVP и т.п.
Access Triple: «Субъект – программа TP – объект CDI»

Внесение изменений только через TP. IVP поддерживает внутреннюю и внешнюю согласованность и разделение обязанностей.

Модель «не влияния» – управление целостностью

Модель «не влияния» – модель управления целостностью. Действия, происходящие на верхнем уровне, не влияют на сущность внизу. Обеспечивает защиту от «Interference Attack» атак.

Модель сетки «Lattice»

Модель сетки «Lattice» – модель защиты, построенная на основе групп.

Brewer & Nash «Китайская стена»

Brewer & Nash «Китайская стена» – модель управления доступом и защиты конфликтов интересов. Построенная на модели «информационных потоков». Основной принцип:

Если пользователь имеет доступ к данным «А», то автоматически запрет на доступ к данным «Б»

Модель Graham – Denning – управление целостностью

Модель Graham – Denning – модель управления целостностью. Опирается на набор прав (8 команд), которые субъект может выполнить над объектом. Список команд:

- Create object
- Create subject
- Delete
- Read rights
- Provide & delete rights

Модель Harrison Ruzzo Ulman

Модель Harrison Ruzzo Ulman – модель управления правами доступов субъектов.

Дискретное Управление Доступом (Discretionally Access Control DAC)

Дискретное Управление Доступом (Discretionally Access Control DAC) – управление доступом на основе списков управления доступом (ACL). Обычно является задачами администратора. Относительно простое в плане администрирования. Требуется высокий уровень формализации организации.

Мандатное Управление Доступом (Mandatory Access Control MAC)

Мандатное Управление Доступом (Mandatory Access Control MAC) – управление доступом на основе меток доступа. К таким меткам могут относиться метки «секретно», «конфиденциально», принадлежность к проекту или функции и т.п. Обычно управляется владельцем. Относительно простое в плане реализации и безопасности. Сложно управлять в централизованной модели и требует высокий уровень осведомленности владельцев ресурсов. Основаны на модели защиты конфиденциальности «Bell La Padula».

Ролевое Управление Доступом (Role Based Access Control RBAC)

Ролевое Управление Доступом (Role Based Access Control RBAC) – управление доступом на основе ролей и членства в группах. Обычно управляется администратором. Является наиболее распространённым в различных современных системах корпоративного управления. Гибкая (гранулярная) система предоставления доступов. Один из недостатков, наличие супер-администратора, с полным доступом к ресурсам и необходимости детальной проработки ролей.

Атрибутное Управление Доступом (Attribute based Access Control ABAC)

Атрибутное Управление Доступом (Attribute based Access Control ABAC) – Представляет из себя предоставление доступов, на основе статических или динамических правил, связанных с атрибутами (времени суток, расположения, членства в группе и т.п.) объекта и субъекта доступа. Основной недостаток – сложность реализации и контроль за состоянием доступа. Наиболее передовая с точки зрения обеспечения информационной безопасности. Также может называться Динамическим Управлением Доступом (Dynamic Access Control DAC).

Уровни доступа

Для управления ИТ активами используется преимущественно модель на основе предоставления контроля по Ролям (Role Based Access Control (RBAC)). Такой подход реализован практически во всех ИТ системах.

Уровни доступа к Информации

Используется комбинированная модель на основе предоставления контроля по Ролям (Role Based Access Control (RBAC)) с Дискретным Распределением прав (Discrete Access Control (DAC)) к файловым ресурсам. Такие возможности реализованы практически во всех современных ИТ системах.

Уровни доступа к Информации (дополнительный)

Для обеспечения более избирательного и доступа к информации и контроля может понадобиться дополнительный специфические ИТ решения с использованием модели (MAC), метки уровня доступа и категорий, а также правил ABAC.

Матрица Контроля Доступов (Access Control Matrix)

Матрица контроля доступов, а также классификация и категоризация объектов (информации) является ключевыми элементами обеспечения Информационной Безопасности.

Требование к процессу управления данными

Различают три основных состояния данных:

- *Данные в покое (Data at rest)* – должны храниться в дата центре компании. Данные должны быть зашифрованы и готовы к использованию в соответствии с матрицей доступов. Должно обеспечиваться надежное хранение, резервирование и архивирование данных.

- *Данные в перемещении (Data in motion)* – должны быть должным образом зашифрованы при передаче на конечные системы

- *Данные в использование (Data in use)* – должны использоваться только на соответствующим подготовленным устройствах и авторизованными пользователями или системами.

Потоки движения информации

Движение информации можно разделить по следующим типам:

Вертикальная (North-South) – Данные перемещаются между уровнями, к примеру, от компании в портфель, из портфеля в компания.

Горизонтальная (West-East) – Данные перемещаются в пределах одного уровня, к примеру, между одной компанией в другую в одном портфеле.

С низу в верх (Bottom-Up) – Направление движения данных с низу в верх, к примеру, от компании в портфель, от портфеля в компания.

С верху в низ (Top-Down) – Направление движения данных с верха в низ, к примеру, от портфеля в компания, от компании в портфель.

Зоны доверия (Trust Zone) – формируются как логические зоны в пределах одной компании (доверительная зона компании), в пределах одного портфеля (доверительная зона портфеля) или компании (доверительная зона компании) или же внешняя (за пределы компании) зона. Зоны доверия могут быть как «горизонтальные» (несколько филиалов одной компании), так и «вертикальные» (несколько компаний одного портфеля).

В зависимости от уровня конфиденциальности (публичные, секретные и т.п.) определены основные критерии и ограничения:

Данные «Общего доступа» могут передаваться от компании в портфель, за пределы компании как горизонтально, так и вертикально в обоих направлениях.

Данные «Внутреннего использования» могут передаваться от компании в портфель, как горизонтально, так и вертикально в обоих направлениях в пределах информационного пространства компании (корпоративная почта, информационная система и т.п.).

Данные «Конфиденциальные» могут передаваться:

горизонтально – внутри компании в обоих направлениях (работник – руководитель при наличии у обоих соответствующего уровня доступа «Конфиденциальные»)

вертикально – в обоих направлениях от компании в портфель, в пределах одной зоны доверия (компания входит в состав портфеля) и наличия соответствующего уровня доступа «Конфиденциальные» у обоих пользователей.

вертикально – в направлении с низу вверх от компании в портфель, в пределах одной зоны доверия (компания входит в состав портфеля) и наличия соответствующего уровня доступа «Конфиденциальные» у пользователя портфеля.

Данные «Конфиденциальные» не могут передаваться:

горизонтально – между компаниями одного портфеля (доверительная зона портфеля) даже при наличии соответствующего уровня доступа «Конфиденциальные» у обоих)

Вертикально – внутри компании в направлении с верху в низ (руководитель – работник при отсутствии у последнего соответствующего уровня доступа «Конфиденциальные»)

вертикально – в направлении с верху вниз, в пределах одной зоны доверия (доверительная зона портфеля) при отсутствии соответствующего уровня доступа «Конфиденциальные» у пользователя в компании.

Данные «Секретные» могут передаваться по указанным для каждого конкретного типа документа порядку следования. Это связано с особыми условиями данного класса документов, перемещение и доступ к которым регламентируется внешними регуляторами. Если конкретно не указан порядок следования, и отсутствуют требования со стороны внешних регуляторов, то данные перемещаются в соответствии с правилами, как и для Конфиденциальные».

Порядок развертывания ИТ инфраструктуры с позиции ИБ

При проектировании, внедрении и сопровождении ИТ сервисов можно рассмотреть следующую модель поведения:



Диаграмма Сценарии ИБ

Базовый сценарий

«Базовый сценарий» – внедрение решения и его конфигурация в соответствии с практиками. Основная мысль – соблюдение принципов «Парето» (20 процентов усилий решают 80 процентов задач). Рассматривается как основной при внедрении ИТ сервисов.

Оптимальный сценарий

«оптимальный сценарий» – в процессе внедрения и сопровождения, можно оптимизировать решение как с точки зрения информационной безопасности, так и с точки зрения оптимизации стоимости.

Параноик

«параноик» – сценарий, при котором делается максимальный уклон в сторону информационной безопасности, даже в ущерб таким важным критериям как стоимость, доступность и управляемость сервиса.

Упрощенный сценарий

«Упрощенный сценарий» – сценарий, при котором некоторые базовые настройки изменяются, что ведет к незначительному снижению информационной безопасности в угоду значительному снижению стоимости или повышенному уровню доступности и управляемости.

Дуракам везет

«дуракам везет» – сценарий, при котором, по каким-либо причинам явно нарушены основные принципы информационной безопасности.

В ИТ системах возможны случаи, когда одна и та же система, при одинаковой стоимости, может быть настроена в соответствии со всеми пятью сценариями. В этом случае процесс развертывания по сценариям (готовые сценарии), должен рассматриваться как механизм реагирования на угрозы информационной безопасности. Для этого создается несколько сценариев готовности всех ИТ сервисов, и при повышении на пример уровня активности хакеров или общего фона ИБ, все системы ИТ инфраструктуры переходят с «базового» сценария на «оптимальный».

Условия совершения компьютерных преступлений

При проектировании и анализе Информационной Безопасности рекомендуется учитывать совпадения следующих условий, необходимых для совершения преступления:

Мотив (Motive – WHY)

Мотив (Motive – WHY). Мотивация для совершения преступления. В качестве мотиваций может служить недовольство сотрудников, получение финансовой прибыли и т. п. Как пример, можно предположить недовольство системного администратора условиями работы и т. п.

Условия (Means – HOW)

Условия (Means – HOW). Наличие необходимых условий, для совершения преступления. Подразумевается наличие технических возможностей для совершения действий. Так, например, системный администратор имеет возможность по смене пароля пользователя и затем просмотр его почты. Наличие мотива и условий, не достаточны для совершения преступления.

Возможности (Opportunity – WHEN+WHERE)

Возможности (Opportunity – WHEN+WHERE). Совпадение благоприятных условий для совершения преступления. Так для нашего примера, отсутствие политик по смене пароля, профилактика, отсутствие систем сбора и обработки логов и т.п.

Система мониторинга и отчетности должна быть внедрена на всех стадиях процесса управления данными.

Контроли управления по защите информации

Общие положения

Для успешного внедрения комплекса решений по информационной безопасности, не менее важным аспектом является внедрения контролей управления. К таким контролям можно отнести следующие категории:

Административные (Administrative) – административные меры по обеспечению информационной безопасности

- Наличие документов в области информационной безопасности
- Соблюдение требования информационной безопасности
- Проведение обучения и семинаров для сотрудников организации

Физические (Physical) – физические элементы по обеспечению информационной безопасности

- Физическая безопасность помещений дата центра
- Физическая безопасность серверов
- Физическая безопасность рабочих компьютеров

Технические (Technical/Logical) – технические аспекты по обеспечению информационной безопасности

- Контроль за физическими носителями информации (шифрование носителей),
- Включение персонального фаервола
- Установка средств антивирусной защиты

Механизмы обеспечения информационной безопасности

•*Превентивные (Preventive)* – механизмы, призванные предотвратить инциденты ИБ

•*Восстановительные (Reductive)* – механизмы, принятые заранее, что может минимизировать риски

•*Детективные (Detective)* – механизмы, призванные как можно скорее определить, что инцидент имел место

•*Репрессивные (Repressive)* – механизмы, применяемые в ответ на повторяющиеся или продолжающиеся инциденты

•*Корректирующие (Corrective)* – механизмы восстановления и т.п.

Контроли (активные меры противодействия) могут быть разбиты на следующие функции (фазы):

•*Директивный (Directive)* – команды и информирование по предотвращению появления угроз (плакаты, предупреждения).

•*Превентивные (Preventative)* – обеспечивают предотвращение появления угроз.

•*Сдерживающие (Deterrent)* – создают сдерживающие факторы, предотвращающие появление угрозы

•*Детективные (Detective)* – определяют угрозу, имеющуюся в вашей системе

•*Корректирующие (Corrective)* – обеспечивают снижение воздействия угрозы

•*Восстановительные (Recovery)* – обеспечивают восстановление элементов безопасности.

Как пример наличие отказоустойчивости и т.п.

•*Компенсующие (Compensatory)* – обеспечивают снижение воздействия угрозы, если она все же имела место.

Preventative		Detective	Corrective	Compensatory
Security Awareness		System Monitoring	OS Upgrade	Backup Generator
Training				
Firewall		IDS	Backup	Hot Site
Anti-virus		Anti-virus	Anti-virus	Server isolation
Security Guard		Motion Detection	Vulnerability Mitigation	
IPS		IPS		

На приведенной таблице показаны основные четыре фазы и какие меры и технические решения можно отнести к какой из них:

Кроме этого необходимо оценивать контроли по следующим атрибутам:

•*Сложность (Complexity)* – какова сложность обхода контролей. В качестве сложностей могут выступать технические, физическая, материальная и т.п. сложность.

•*Доступ (Access)* – Какие доступы необходимо получить для обхода контроля

•*Привилегии (Privilege)* – какие привилегии (возможности) получит преступник, при обходе контроля.

Методы проведения теста на проникновение

Проведение теста на проникновение позволяет оценить состояние информационной безопасности организации, как с технической точки зрения, так и с точки зрения готовности сотрудников и процессов организации. Тестирование может проводиться для проверки как конкретного решения (интернет банкинга, сайта и т.п.), готовности сотрудников департаментов ИТ и Безопасности (Red Team Testing), или всей организации. Обычно проводится с привлечением компаний, имеющих опыт по проведению данных тестов, классифицированный персонал, методику и технические средства. В качестве методик проведения теста на проникновение могут быть использованы:

OISSG

OSSTMM

NIST Guideline on Network Security Testing

ISACA Testing IT Systems Security

Cybersecurity VAMs

OWASP Testing Guide

Собственные методики

Основные десять видов угроз по спецификации OWAST top 10:

Injectons

Broken Authentication & Session Management

CSS / XSS

Insecure Direct Object References

Security Misconfiguration

Sensitive Data Exposure

Missing Function Level Access Control

CSRF / XSRF – Подделка межсайтового запроса

Using components with known vulnerabilities

Invalidated Redirects & Forwarding

Резервное копирование и архивирование данных

Политики резервного копирования и архивирования одни из важнейших элементов защиты данных в организации.

Классическое правило резервного копирования и архивирования данных известное как «3-2-1» подразумевает:

- Наличие трех (3) копий данных расположенных в разных местах
- Наличие двух (2) форматов / состояний данных
- Как минимум одна (1) копия данных располагается за пределами офиса

Следующее важное правило, которое необходимо соблюдать:

- Тестирование целостности файла резервного копирования или архива
- Тестирование возможности восстановления на целевой системе

Для грубого расчета объема для резервного хранилища можно принимать соотношение «Дата – Бэкап» 1:3.

Существуют следующие стратегии ротации резервных носителей при создания резервных или архивных копий:

Пользовательский (Customer)

Пользовательский (Customer) стратегия резервное копирование – выполняемое вручную обычно полная копия. Используется обычно перед внесением изменений. Требуется одна операция (создание или восстановление).



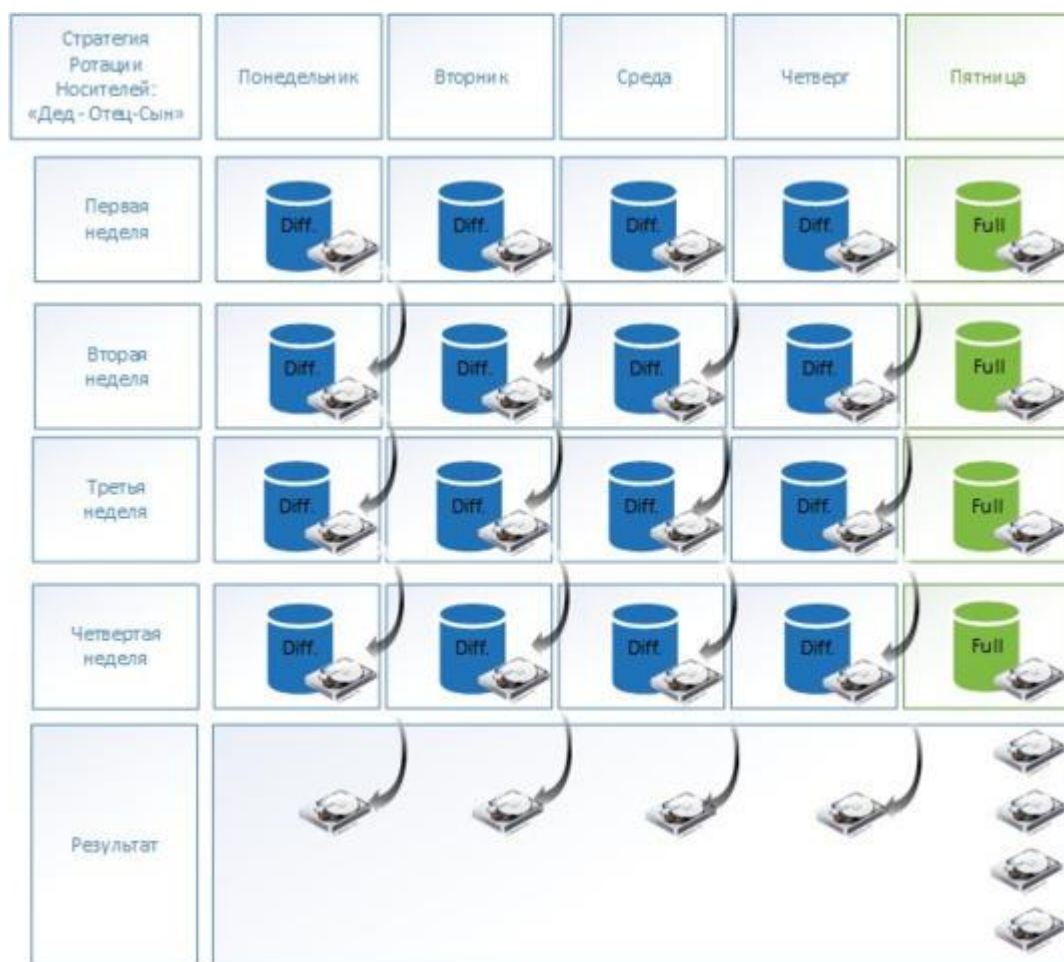
«Дед – отец – сын» («Grandfather – Father – Son» GFS)

«Дед – отец – сын» («Grandfather – Father – Son» GFS) стратегия резервное копирование – выполняемая автоматически или полуавтоматически. Используется обычно по расписанию.

«Сын» – Ежедневная полная резервная копия данных на один носитель (файл, контейнер). Период защиты данных – дата последней резервной копии. Требует один носитель (контейнер) информации.

«Отец» – Предполагает наличие недельной полной резервной копия данных и ежедневных дифференциальных или добавочных копий данных. В качестве периода защиты выбирается двух недельный период. Требуется наличие минимум шести (6) носителей (контейнер) информации. Позволяет восстановить данные каждой недели (2) и ежедневные данные последней недели (4).

Стратегия может быть рассчитана на месячный цикл. Для этого понадобится восемь (8) носителей информации: Позволяет восстановить данные конца месяца (1), еженедельные данные месяца (3) ежедневные данные последней недели (4).



«Дед» – Предполагает наличие месячной и недельной полной резервной копия данных и ежедневных дифференциальных или добавочных копий данных. В качестве периода защиты выбирается годовой период. Требуется наличие минимум девятнадцати (19) носителей (контейнер) информации. Позволяет восстановить данные каждого месяца (12), еженедельные данные последнего месяца (3) ежедневные данные последней недели (4).

Ежедневный полный (Daily Full Backup)

Ежедневный полный (Daily Full Backup) стратегия ежедневного полного резервного копирования данных с последующим сохранением. Требуется наличие порядка (365) носителей (контейнер) информации или по количеству рабочих дней. Обычно применяется в финансовых организациях.



«Ханойская башня» («Tower of Hanoi»)

«Ханойская башня» («Tower of Hanoi») стратегия резервное копирование – выполняемая автоматически или полуавтоматически. Используется обычно по расписанию. Требует наличие нескольких наборов носителей данных. Количество наборов не регламентируется, но принимается обычно пять шесть комплектов.

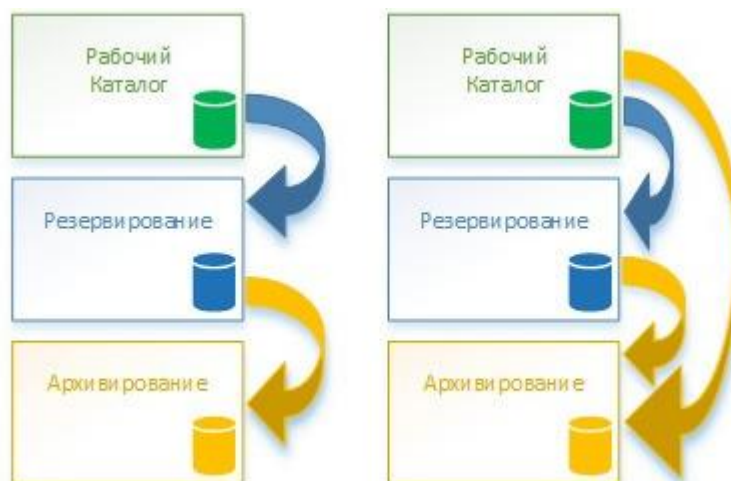
«Стратегия 10 наборов»

«Стратегия 10 наборов» – стратегия резервное копирование – выполняемая автоматически или полуавтоматически. Используется обычно по расписанию. Требует наличие десяти наборов носителей данных из расчета сорока (40) недельного периода обращения. За каждым набором закрепляется один день недели. С каждым циклом происходит сдвиг наборов (например, если набор N1 закреплен за понедельником, набор N2 за вторником, то при смене цикла набор N1 сдвигается на вторник и т.п.).

Последние две стратегии используются редко, в связи со спецификой работы и поддержки со стороны систем резервного копирования. Основная причина их использования была продиктована неравномерностью использования ленточных носителей информации, имеющих ограниченное количество операций записи-чтения. При применении Систем Резервного Хранения Данных (СРХД) на основе дисков, данная проблема потеряла актуальность.

Еще одним из важных моментов политики резервирования и архивирования является совместное использование политик резервного копирования и архивирования. Возможные варианты комплексного подхода:

- Каскадная – соблюдается последовательность: «Рабочий каталог – Резервная копия – Архивная копия»
- Независимая – рабочий каталог может являться одновременно источником для резервного копирования, так и архивирования.



Независимая модель позволяет соблюдать правило «3-2-1». Данные одновременно хранятся в двух разных местах и в различных форматах. Например, резервная копия хранится жестких дисках системы резервного хранения данных, а архивная копия на ленточных носителях. К недостаткам данной модели можно отнести необходимость более длительного окна для создания сначала резервной, а затем архивной копии.

Каскадная модель позволяет уменьшить время работы с рабочими данными, делая только резервное копирование. Архивирование может происходить в рабочее время, не затрагивая рабочие каталоги данных. Кроме этого происходит два процесса с одними данными, что увеличивает вероятность ошибки как при создании, так и при восстановлении, а также требует совместимость систем.

Порядок восстановления данных может быть одинаковый. Кроме всего выше сказанного, необходимо отметить следующие аспекты:

- современные системы хранения позволяют переносить редко используемые данные на более дешевые носители информации, тем самым уменьшая объем рабочего каталога, что ведет в свою очередь к уменьшению как времени резервирования, так и требуемых объемов.

- Продумать отказоустойчивость самих систем резервирования и архивирования.

Политика резервного копирования и восстановления данных (Backup & Recovery Policy)

Политика резервного копирования одна из важнейших элементов защиты данных в организации.

Для формирования грамотной политики резервного копирования необходимо определить ряд входных параметров:

Источник данных

Тип данных

- Состояние системы, сервиса или сервера
- Конфигурация
- Данные
- Логи событий или аудита

Объем данных – максимальный объем данных

Утилизация данных

- используемый объем данных,
- характер поведения
- прирост данных за определённый период

Объем изменений – характер изменений данных и предполагаемый объем измененных данных

Окно для проведения резервного копирования – отрезок времени для выполнения резервного копирования

Требуемые характеристики:

- *Объект Восстановления (Recovery Point Objective RPO)* – целевая точка восстановления, определяющая объем данных или времени допустимый для потери (дневные изменения и т.п.)
- *Время Восстановления (Recovery Time Objective RTO)* – целевое время восстановления, определяющее время, необходимое для восстановления данных или сервиса.
- *Уровень Восстановления (Recovery Level Objective RLO)* – целевой уровень восстановления, определяющий на каком уровне необходимо восстановить данные или систему (например, восстановление состояния сервера или сервиса, восстановление данных СУБД или файлов, частичное или полное восстановление).
- *Триггер срабатывания* – механизмы включения резервного копирования: по расписанию, по изменениям.

На основе входных данных можно выбрать правильное техническое решение. Существуют следующие опции создания резервных копий:

Полное (Full Backup) резервное копирование – обеспечивает резервное копирование всей информации. Характеризуется долгим временем создания и восстановления. Требуется одна операция (создание или восстановление).

Резервное копирование накопленных изменений (Differential Backup) – обеспечивает резервное копирование информации изменившейся с момента создания полной резервной копии. Характеризуется относительно коротким временем создания и восстановления. Требуется две операции для восстановления (восстановление полной версии и изменений).

Резервное копирование добавочных или дневных данных (Incremental or Daily Backup) – обеспечивает резервное копирование информации изменившейся с момента создания последней резервной копии изменений. Характеризуется коротким временем создания и восстановления. Требуется 1 + N операций для восстановления (восстановление полной версии и последовательное восстановление всех изменений до необходимого момента).

Полная копия (Full Copy Backup) резервное копирование – обеспечивает резервное копирование всей информации, без изменения атрибута архивирования файлов. Характеризуется долгим временем создания и восстановления, но требуется одна операция (создание или восстановление). Производится в любой момент времени и не влияет на организацию процесса резервного копирования.

Композитное (Composite Backup) резервное копирование – обеспечивает резервное копирование изменений с возможностью создания полной резервной копии на любой момент времени. Характеризуется быстрым временем создания и восстановления. Обычно является функциональной возможностью специализированных программно-аппаратных решений по резервному копированию.

Политика резервного копирования должна обеспечивать выполнение следующих требований:

- Тип и частота резервного копирования зависит от бизнеса, требований и функциональных особенностей сервиса
- Тип и скорость восстановления зависит от бизнеса, требований и функциональных особенностей сервиса
- Ежедневное резервное копирование данных сервиса. Может включать в себя различные уровни, такие как резервное копирование целиком виртуальных машин, так и/или данных.

Политика восстановления данных (Recovery Policy)

Политика восстановления данных описывает организацию обратного процесса, а именно, восстановления данных. Политика должна описывать триггеры, запускающие процесс восстановления, уровень восстановления данных (на уровне сервера, приложения и т.п.), тип восстановления (полное или частичное). Кроме этого должны быть определены методы и временные рамки.

Пример расчета объема резервной копии данных

Полезный объем характеризует возможность восстановить данные за последнюю неделю.

Полный объем характеризует возможность восстановить данные за месяц и необходимое для этого пространство.

Рабочий объем характеризует коэффициент заполнения диска на 60%.
Резервная копия виртуальной машины по умолчанию выполняется по схеме:
5 Last Days (Differential) +1 Last Week (Full) + one Current Month (Full)

Дневной (D) – Различный (Differential Backup) 5 дней (понедельник-пятница): $5 \times 1 \text{ MB} = 5 \text{ MB}$ один сервер.

Еженедельный (W) – Полный (Full Backup) 1 день (суббота): $1 \times 60 \text{ GB} = 60 \text{ GB}$ один сервер.

Ежемесячный (M) – Полный (Full Backup) 1 день (конец месяца): $1 \times 60 \text{ GB} = 60 \text{ GB}$ один сервер.

Полный объем резервной копии сервера за месяц: $25D + 5W + 1M = 75 \text{ MB} + 300 \text{ GB} + 60 \text{ GB} = 435 \text{ GB}$

Полный Рабочий объем резервной копии с коэффициентом заполнения диска 60%: $435 \text{ GB} \times 0.6 = 261 \text{ GB}$

Полезный объем резервной копии сервера: $5D + 1W + 1M = 5 \text{ MB} + 60 \text{ GB} + 60 \text{ GB} = 125 \text{ GB}$

Полезный Рабочий объем резервной копии с коэффициентом заполнения диска 60%: $125 \text{ GB} \times 0.6 = 75 \text{ GB}$

Резервная копия данных по умолчанию выполняется по схеме:

5 Last Days (Incremental) +1 Last Week (Full) + one Current Month (Full)

Для расчета на каждые 100GB данных при 10% изменениях (10GB) и 60% заполнением диска:

Дневной (I) – Различный (Incremental) 5 дней (понедельник-пятница): $5 \times 10 \text{ GB} = 50 \text{ GB}$ один сервер.

Еженедельный (W) – Полный (Full Backup) 1 день (суббота): $1 \times 100 \text{ GB} = 100 \text{ GB}$ один сервер.

Ежемесячный (M) – Полный (Full Backup) 1 день (конец месяца): $1 \times 100 \text{ GB} = 100 \text{ GB}$ один сервер.

Полный объем резервной копии сервера за месяц: $25I + 5W + 1M = 250 \text{ GB} + 500 \text{ GB} + 100 \text{ GB} = 850 \text{ GB}$

Полный Рабочий объем резервной копии с коэффициентом заполнения диска 60%: $850 \text{ GB} \times 0.6 = 510 \text{ GB}$

Полезный объем резервной копии сервера: $5I + 1W + 1M = 50 \text{ GB} + 100 \text{ GB} + 100 \text{ GB} = 250 \text{ GB}$

Полезный Рабочий объем резервной копии с коэффициентом заполнения диска 60%: $250 \text{ GB} \times 0.6 = 150 \text{ GB}$

Для восстановления данных необходимо 390GB, для хранения резервных копий данных необходимо 590GB.

Общий полный рабочий объем пространства для хранения резервной копии сервера и данных $261 \text{ GB} + 510 \text{ GB} = 771 \text{ GB}$

Общий полезный рабочий объем пространства для хранения резервной копии сервера и данных $75 \text{ GB} + 150 \text{ GB} = 225 \text{ GB}$

Политика архивирования данных (Data Archiving Policy)

Политика архивирования данных является дополнительным элементом защиты данных. Должна обеспечивать возможность длительного хранения данных и безапелляционно подтверждать, что данные не были модифицированы с момента их создания. Решение может обеспечивать архивирование резервных копий, или же самостоятельное создание резервной копии с последующим архивированием данных.

Политика архивирования данных должна обеспечивать выполнение следующих требований:

- Тип и частота архивирования данных зависит от бизнеса требований и функциональных особенностей сервиса

- Архивные копии данных должны быть зашифрованы.

- Безапелляционно доказывать неизменность данных с момента создания

- Обеспечивать долгосрочное хранение информации

- Обеспечивать возможность хранения вне организации, и вне ИТ инфраструктуре (внешние носители)

Пример расчета объема архивирования данных

Архивирование резервных копий серверов в течении 3 месяцев. Архивирование по умолчанию выполняется по схеме:

2 Months (previous months Full Backups)

Полный Рабочий объем пространства для хранения архивной копии виртуальной машины 2 x 72GB+261GB = 405GB

Полный Рабочий объем пространства для хранения архивной копии данных 2 x 60GB+510GB = 630GB

Полезный Рабочий объем пространства для хранения архивной виртуальной машины 75GB +2 x 36GB = 147GB

Полезный Рабочий объем пространства для хранения архивной копии данных 150GB +2 x 60GB = 270GB

Общий полный рабочий объем пространства для хранения архивной копии сервера и данных 405GB+630GB = 1035GB

Общий полезный рабочий объем пространства для хранения архивной копии сервера и данных 147GB+270GB= 417GB

Политика устаревания активов (Retention Policy)

Политика устаревания активов описывает организацию процесса удаления данных и списания ИТ активов. Основные цели политики:

- высвобождение мощностей хранилищ данных
- вывод из эксплуатации сервисов, сопровождение которых не целесообразно и не отвечающих требованиям бизнеса
- поддержка актуальных данных и сервисов и оптимизация процесса управления ИТ сервисами
- высвобождение вычислительных мощностей для новых технологий и сервисов

Политика должна обеспечивать классификацию активов, описывать процесс определения устаревания активов, безопасное удаление данных в установленные сроки и надежными методами.

Технические аспекты Информационной Безопасности

Общие положения

Система защиты информации является комплексным / много уровневый решением, обеспечивающим защиту информации и ИТ активы компании. Для успешного обеспечения информационной безопасности необходимо ввести понятия классификации информации и ИТ активов (уровень конфиденциальности), наличие политик и процедур, средств мониторинга, обучения персонала и т.п. Системы могут включать весь требуемый функционал в одном программно-аппаратном решении (бюджетный вариант) так и разнесенным по разным устройствам. Выбор решения зависит от требований, особенности работы и финансовых возможностей организации. К системам защиты информации относятся следующие системы и компоненты:

Системы защиты периметра:

Брандмауэр (Firewall)

Системы Аутентификации и контроля доступа (ACL)

Система фильтрации веб трафика (Web Security Gateway)

Прокси сервер (Forward Proxy Server)

Обратный прокси сервер (Reverse Proxy Server)

Система обнаружения / предотвращения вторжения (IDS/IPS)

Системы защиты от вирусов и зловредных программ (Antivirus)

Системы защиты почтовых систем от спама (SPAM filter)

Системы защиты веб контента (WAF)

Система балансировки нагрузки (Load Balancer)

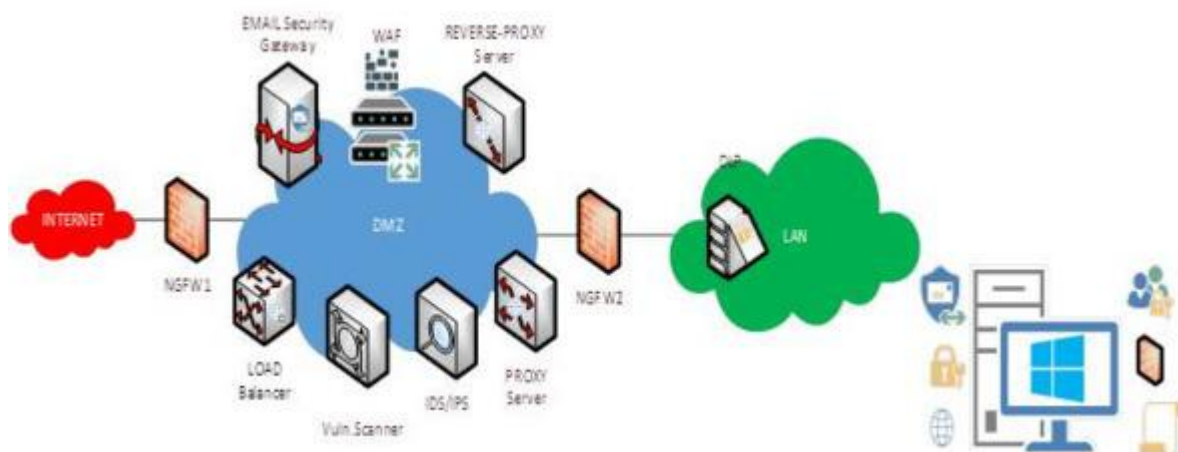
Система сканирования на поиск уязвимостей (Vulnerability Scanner)

Системы предотвращения утечки данных (DLP)

Система Управления Правами Доступов (Right Management System)

Система Идентификации Пользователей (Identity Management System)

Системы защиты конечных устройств (Personal Firewall/Antivirus):
Персональный Брандмауэр (Personal Firewall)
Системы защиты от вирусов и зловредных программ (Antivirus)
Системы шифрования жестких дисков и съёмных носителей (BitLocker, NTFS/EFS)
Отсутствие «Административного» уровня доступа для всех пользователей систем, принцип «минимальных» привилегий
Системы контроля приложений



Компоненты информационной безопасности могут являться как функциональными элементами фаервол, так и отдельными решениями.

Требования к защите локальной сети и систем

Департамент Безопасности должен обеспечивать физическую защиту ИТ активов, как дата центра, так и системы конечных пользователей.

Для каждой компании и портфеля могут формироваться свои дополнительные требования и методы защиты с учетом конкретной реализации. Данная задача является ключевой для подразделения Информационной Безопасности.

Физический уровень

Ограничивается доступ к ключевым элементам сети (коммуникационные шкафы, сетевое оборудование и т.п.)

Не используемые рабочие точки конечных пользователей блокируются (либо не подключаются к коммутатору, либо блокируются на коммутаторе)

Физическая изоляция гостевой сети беспроводного соединения (Guest Wi-Fi isolation).

При использовании персональных устройств (телефонов, планшетов и т.п.) в корпоративной сети, обязательно включение механизма 802.1X и WPA2-Enterprise.

Использовать средства мониторинга сети на предмет работы «не авторизованных» DHCP серверов по специфике отклика и значению TTL.

Контроль или блокировка локальных портов и устройств серверов и конечных пользователей.

Использование пароля на доступ к BIOS серверов и конечных пользователей.

Шифрование устройств хранения данных (дисков) серверов и конечных пользователей.

Канальный уровень

Сегментирование сети на канальном уровне (Виртуальные сети)

Обеспечивается защита портов коммутатора (Port Security). На каждый порт коммутатора привязывается аппаратный адрес устройства (MAC address) или группы устройств, имеющих возможность, подключаться. Или статическая таблица на коммутаторе (CAM)

Включается связка сервера динамической раздачи сетевых адресов (DHCP snooping). Явное указание на коммутаторе на каком порте отвечает авторизованный DHCP сервер.

Инспекция механизма разрешения адресов (ARP inspection). Контроль и мониторинг связки сетевого адреса и аппаратного адреса устройства (MAC address – IP address).

Защита источника (Source Guard). Дополнительный механизм защиты, обеспечивающий привязку MAC address – IP address к интерфейсу коммутатора.

Сетевой и транспортный уровень

Контроль маршрутизации и настройка доступов по правилу «только разрешено»

Использовать для обращения в сети только имена ресурсов (FQDN) вместо сетевых адресов. Тем самым принудительно инициируется использование Kerberos протокола для систем на базе Microsoft Windows.

Блокировать использование протоколов и механизмов ниже чем NTLM v2. Возможно использование групповых политик для выполнения данных задач

Блокировка механизма WPAD. Для реализации необходимо через групповые политики запретить авто-обнаружения прокси и протокола LLMNR, или же назначение статической записи. Установить «заглушку» в DNS сервере на WPAD запись (WPAD.domain.name).

Отключение протокола NetBIOS.

Отключение скрытых ресурсов ADMIN\$, C\$, D\$ и т.п. для систем на базе Microsoft Windows. Возможно через групповые политики.

Активировать возможности систем безопасности на серверах и конечных устройствах (антивирус, фаервол и т.п.)

Отключение на системах конечных пользователей систем на базе Microsoft Windows сервиса «Предоставления файлов и печати для совместного пользования»

Не создавать локальные учетные записи администраторов через механизм групповых политик для систем на базе Microsoft Windows.

Использовать доменные учетные записи для локальных групп администраторов для систем на базе Microsoft Windows.

Требования к пропускной способности (минимальная, максимальная, ожидаемая)

управления адресами сети

Контроль трафика

Шифрование трафика критически важных приложений и систем

Ведение лога активности

Корпоративная сеть отделена от публичной сети (интернета) по средствам Демилитаризованной зоны (DMZ)

Корпоративная сеть защищена по периметру техническими средствами и решениями, такими как фаервол (Next Generation Firewall (NGFW))

При необходимости фаервол защиты веб приложений (Web Application Firewall (WAF))

Системы Обнаружения и Предотвращения Вторжения (Intrusion Detection and Intrusion Prevention Systems (IPS/IDS)) должны быть соответственно настроены

Ресурсы публикуемые наружу должны быть размещены в Демилитаризованной зоне (DMZ)

Корпоративная сеть должна быть правильно сегментирована с учетом уровня портфелей и компаний

Сетевые устройства настроены с учетом безопасности для периферийных устройств, и с учетом производительности для внутренних устройств

Только необходимые сервисы должны быть запущены, и разрешенные протоколы и порты настроены на данных устройствах

Трафика между клиентом и сервером должен шифроваться
Все сетевые устройства должны быть своевременно обновляться
При необходимости развернут комплекс мер по Защите от Утечки Данных (Data Leakage / Loss Prevention (DLP))
Необходимый мониторинг активности и состояние сети должен вестись с возможностью предоставления отчетности

Требование к серверам и инфраструктуре виртуализации и систем хранения

Все сервера должны быть своевременно обновлены (обновления, прошивки)
На всех серверах должны быть включены и настроены локальные фаерволы
На все сервера должны быть установлены средства антивирусной защиты
Корпоративная сеть должна быть правильно сегментирована с учетом уровня портфелей и компаний
Серверный сегмент отделен от сегмента клиентов
Только необходимые сервисы должны быть запущены, и разрешенные протоколы и порты настроены на данных устройствах
Трафика между клиентом и сервером должен шифроваться
При необходимости развернут комплекс мер по Защите от Утечки Данных (Data Leakage / Loss Prevention (DLP))
Необходимый мониторинг активности и состояние серверов должен вестись с возможностью предоставления отчетности

Требование к системам конечных пользователей

Все системы конечных пользователей должны быть частью леса
На все системы конечных пользователей должны входить с учетными данными леса
Локальные диски всех систем конечных пользователей должны быть зашифрованы
Порты ввода / вывода (DVD, USB etc.) всех систем конечных пользователей должны быть под контролем или же деактивированы
Все системы конечных пользователей должны быть своевременно обновлены (обновления, прошивки)
На всех системах конечных пользователей должны быть включены и настроены локальные фаерволы
На все системах конечных пользователей должны быть установлены средства антивирусной защиты
На все системах конечных пользователей должно быть установлено только разрешенное программное обеспечение
Пользователи не должны знать или использовать учетные записи с повышенными привилегиями
Только необходимые сервисы должны быть запущены, и разрешенные протоколы и порты настроены на данных устройствах
Трафика между клиентом и сервером должен шифроваться
При необходимости развернут комплекс мер по Защите от Утечки Данных (Data Leakage / Loss Prevention (DLP))
Необходимый мониторинг активности и состояние систем конечных пользователей должен вестись с возможностью предоставления отчетности

Все системы и компоненты информационной безопасности должны по возможности тестироваться на возможность выполнения атаки, с использованием различных инструментов, в том числе и выделенных инструментов таких как «Ixia Breakpoint».

Уровень приложений

Не выключать механизма UAC для систем на базе Microsoft Windows.

Не предоставлять права локальных администраторов пользователям.

Использование «сервисных» учетных записей для запуска сервисов и служб для систем на базе Microsoft Windows.

Запрет на установку программного обеспечения локально, и из папок TEMP, TMP, App Data.

Производить установку программного обеспечения только через групповые политики или специализированные решения.

Внедрение групповой политики RESTRICTED GROUPS для членов группы локальных администраторов.

Переименование учетных записей администраторов.

Внедрение механизма AppLocker для систем на базе Microsoft Windows.

Внедрение механизма EMET для систем на базе Microsoft Windows.

Внедрение механизма LAPS для систем на базе Microsoft Windows.

Включение параметров «Force GPO to reapply settings during refresh» для систем на базе Microsoft Windows.

Отключение не используемого функционала и служб.

Отключение механизма «Net Session Enumeration» для систем на базе Microsoft Windows.

Отключение механизма «Windows Browser Protocol» для систем на базе Microsoft Windows.

Отключение механизма WSH для систем на базе Microsoft Windows.

Отключение возможности локальных администраторов аутентифицироваться по сети «Prevent Local Admins (RIP500) to authenticate over network» для систем на базе Microsoft Windows.

Блокировка не доверенных шрифтов для систем на базе Microsoft Windows.

Внедрения механизма «Credential Guard» для систем на базе Microsoft Windows.

Внедрение механизма «Device Guard» для систем на базе Microsoft Windows.

Отключение или контроль возможностей «Macros» и «OLE» in Microsoft Office».

Настройка механизма аутентификации «Restrict Unauthenticated RPC client» для клиентов для систем на базе Microsoft Windows.

Настройка механизмов «классификации файлов и данных» файловых серверов и систем на базе Microsoft Windows.

Внедрение механизмов контроля привилегий (Privileges Access Management PAM) и его элементов: достаточности привилегий (Just Enough Administration JEA) и ограниченности по времени (Just In Time Privileges JIT).

Таблица угроз и видов атак

Denial of Service DoS

Dynamic Denial of Service DDoS

Flood – «Затопление». Различаются SYN Flood, ICMP Flood, DNS Flood

Bonk, Teardrop, Pong – Фрагментированные пакеты больших размеров приводящие к переполнению буфера и отказу систем.

SMURF – Ошибки реализации стека протокола TCP/IP.

Ping of DEATH (Jolt, SSPing)

UDP Storm – Шторм пакетов, настраивается как пересылка пакетов между двумя открытыми портами.

UDP Bomb – Некорректный UDP пакет.

LAND – Отправка пакета на определённый порт, но отправитель указывается тот же самый.

Mail Bombing

Sniffing – Прослушивание сети.

IP Hijack – Физическое или логическое «врезание» в канал связи.

Dummy DNS Server – Ложный DNS сервер.

Fuzzy – Подделка пакетов.

Puke – Фабрикует пакеты ответа ICMP unreachable на клиенте.
Fake unreachable – Тоже самое, что и Puke, но направлен на сервер.
Host spoofing – Подмена хоста
Password crack – Атаки направленные на взлом или перебор пароля.
Back connect / Pipes /Reverse
Software Vulnerabilities
Buffer Overflow – Использование ошибки переполнения буфера.
Shatter
Nuke – Атака на протокол NetBIOS (TCP, UDP 137, 138, 139).
Cross User Attack
CGI Attack
SQL Injection – Инжекция в SQL запросы
HTTP Resource Splitting (HRS)
Cross User Defacement
Web Cache Poisoning / Browser Cache Poisoning
Hijacking Pages
Cross Site Scripting / Exchange Site Scripting (CSS / XSS)
SQL Injection CSS (CIXSS)
SQL Injection HTTP Resource Splitting (SiHRS)
NULL Bute (Perl) – Специфика атак с использованием Perl
Include bute, PHP Include bute – Специфика атак на PHP
Hidden Fields
Man in the Middle Attack (MITM) – Атака через посредника.
Man in the Browser Attack (MITB) – Атака на Интернет банкинг

Заключение

К сожалению, на практике достаточно часто бизнес считает, что вопросами информационной безопасности должна заниматься только ИТ. Еще хуже, когда бизнес не понимает, зачем вообще нужно уделять внимание информационной безопасности. Создание эффективной системы защиты информации влечет за собой большие затраты, которые должны быть понятны руководству, так как именно оно принимает решение о финансировании. При этом важно соблюдать баланс – обеспечение информационной безопасности не должно стоить больше самой защищаемой информации.

Концепция Информационной Безопасности должны принимается в расчет на всех этапах построения и сопровождения ИТ, будь то управление проектами, управления ИТ сервисами, управления качеством. Приоритеты (доступность или конфиденциальность) должны быть определены на начальном этапе и на самом высоком уровне организации. Порядок взаимодействия ИТ и Безопасности также должны быть описаны на уровне Архитектуры Предприятия. В целом, статистика который год однозначно показывает, основные инциденты и угрозы информационной безопасности, в более чем семидесяти процентах случаях, происходили не по техническим причинам, а из-за ошибок сотрудников, недостатка знаний и квалификации, намеренных действий «инсайдеров», а также не соблюдения требований информационной безопасности сотрудниками организаций. Поэтому главные аспекты обеспечения информационной безопасности:

- жесткая дисциплина
- непрерывное обучение и периодическое тестирование всех сотрудников организации без исключения
- контроль за изменениями

Концепция Управления ИТ Сервисами

Основные определения

Данный раздел содержит основные принципы управления ИТ сервиса на всем жизненном цикле сервиса. Концепция основывается на стандартах COSO, ITAF, Balanced Score Card, COBIT, ITIL, ISO 20000, ISO27000, ISO 17799, ISO9000, MOF. За основу взята «сервис

ориентированный» подход к управлению ИТ. Процессный подход предполагает представление основных деятельности ИТ в виде процессов, состоящих из действий.

Процесс – структурированный набор видов деятельности, спроектированный для достижения определенной цели. В общем, процесс представляет собой набор процедур, на которые оказывает влияние политика организации и процедур, происходящих из других источников, в том числе процессов. Процессы имеют четкие, обусловленные бизнесом, причины возникновения, ответственных владельцев, должностные обязанности, связанные с наполнением процесса и средства измерения эффективности. Процессы имеют следующие характеристики:

- Процессы измеряемы, то есть можно измерить процесс каким-либо подходящим методом. Менеджеры стремятся измерить в первую очередь стоимость и качество, а практикующие пользователи – продолжительность и продуктивность процесса.

- Процессы служат для достижения конкретных результатов. Причина существования процесса – предоставление конкретного результата, который можно идентифицировать и посчитать.

- Процессы имеют потребителей – каждый процесс предоставляет свои результаты потребителям или другим процессам. Потребители могут быть внутри или вне организации, но процессы в любом случае должны удовлетворять их ожиданиям.

- Процессы состоят из действий. Действие (Activity) – основные виды деятельности, предпринимаемые в рамках процесса.

Не менее важными понятиями являются:

- *Владелец сервиса (service owner)* – роль или структурное подразделение организации, который занимается постановкой целей, принимает решения и управляет финансированием по сервису.

- *Менеджер сервиса (service manager)* – роль или структурное подразделение организации, который занимается выполнением целей и задач, поставленных владельцем сервиса, обеспечивает развертывание и сопровождение сервиса.

Любой менеджер знает, что одна из самых сложных задач управления – построить и заставить работать процессы. Без налаженных процессов получить результаты – это подвиг. Подвиги достойны уважения, если совершаются в первый раз. Постоянные подвиги вызваны управленческой слабостью и ведут к проблемам, стрессам, текучке и плохим результатам. С ростом организации это приведет к гибели компании. Вся деятельность ИТ департамента разбита на процессы. Краткое описание сервисов приводится в данной главе.

Требования бизнеса

Требования бизнеса являются ключевым драйвом при внедрении ИТ решений. Любой сервис должен быть рассмотрен с точки зрения бизнес-ориентирования.

- Бизнес сервисы, имеющие непосредственное влияние на бизнес должны обладать первичным приоритетом.

- Технические сервисы (Корневые, первичные, вторичные и вспомогательные) нацелены на поддержание бизнес сервисов и приложений на надлежащем уровне.

При проектировании систем компании следует руководствоваться:

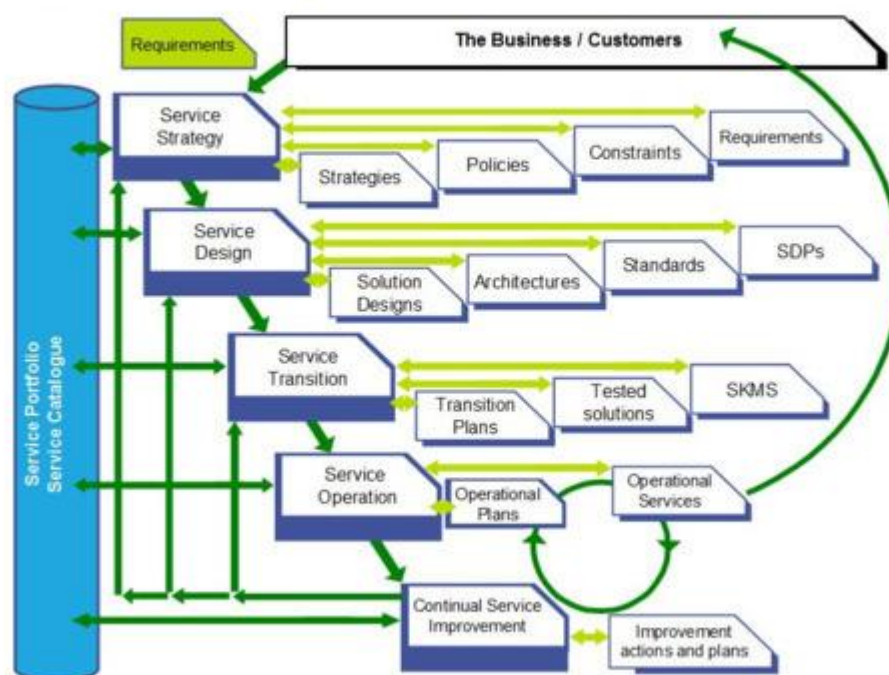
- Определить и следовать цепочке требований: доступность, безопасность и целостность.

- Бизнес сервисы имеют первичный приоритет.

- Технические сервисы (корневые и первичные) имеют первичный приоритет, и рекомендуется рассматривать в контексте максимальной доступности и надежности.

- Технические сервисы (вторичные и вспомогательные) имеют вторичный приоритет, и рекомендуется рассматривать в контексте минимальных расходов.

IT Service Lifecycle



ITIL © is a Registered Trade Mark, and Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

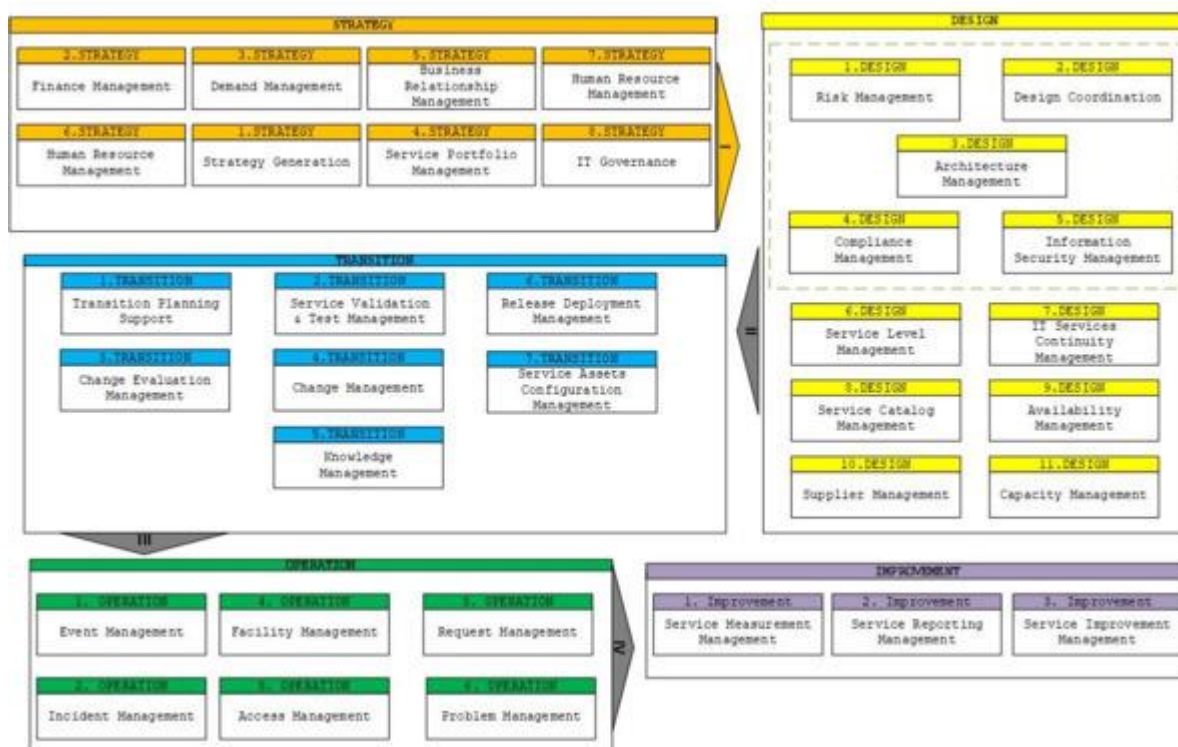
Cloud
Ref: 3C0006

2

Фазы жизненного цикла ИТ сервиса

Согласно ITIL v3 определены следующие этапы (5) управления ИТ сервисами с использованием (26) процессов, (6) функций, а также (2) направления.

ITIL v3 advanced Processes Map



Модели ИТ архитектуры

ИТ архитектура организации может строиться по нескольким моделям:

- «Децентрализованная» – Вычислительные мощности расположены по портфелям или компаниям организации.

- «Централизованная» – Вычислительные мощности расположены в дата центре холдинга, на периферии остаются «front-end» решения и службы поддержки пользователей.

- «Облачная» – Вычислительные мощности переносятся в «облако».

- «Смешанная» – Вычислительные мощности расположены как в дата центре холдинга, так и в облаке.

Модели предоставления ИТ сервисов

ИТ департамент компании ориентирован на предоставление различного уровня услуг. Определены следующие модели:

- Совместное размещение (Co-location IT assets) – ИТ ресурсы компаний размещены в дата центре. ИТ службы компаний самостоятельно управляют данными ИТ ресурсами.

- Инфраструктура как Сервис (Infrastructure as Service (IaaS)) – ИТ департамент предоставляет вычислительные ресурсы и инфраструктуру, которая включает в себя, но не ограничивается сеть, виртуализация, доступ в интернет, хостинг и т.п. ИТ службы компании самостоятельно управляют ИТ ресурсами, расположенными на данных инфраструктурах.

- Платформа как Сервис (Platform as Service (PaaS)) – ИТ департамент предоставляет вычислительные ресурсы, инфраструктуру и платформу, которая включает в себя, но не ограничивается, хостинг, ERP платформа и т.п. ИТ службы компаний самостоятельно управляют ИТ ресурсами, расположенными на данных платформах.

- Программы как Сервис (Software as Service (SaaS)) – ИТ департамент предоставляет вычислительные ресурсы, инфраструктуру, платформу и сами сервисы, которая включает в себя, но не ограничивается, корпоративная почта, Интрасети и т.п. Компании являются пользователями данных услуг.

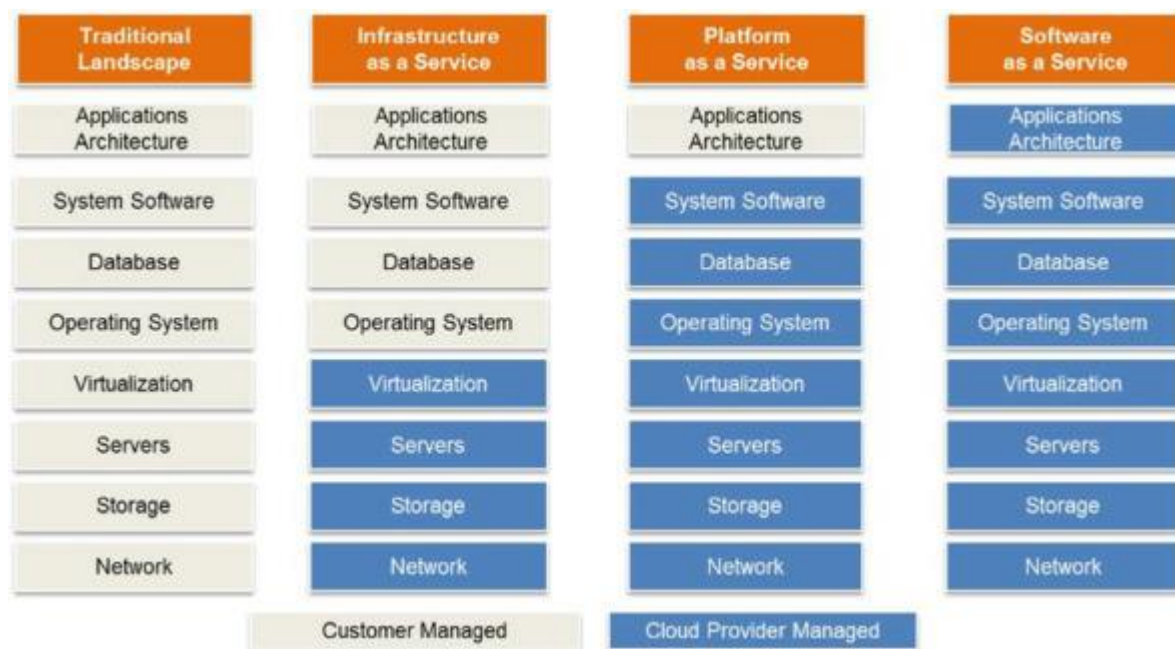


Диаграмма предоставления ИТ сервисов

Типы предоставления сервисов

Типы предоставления сервисов определяются как на стратегическом этапе для ИТ стратегии в целом, так и для каждого сервиса в отдельности. Так в частности, при проектировании бизнес систем необходимо определиться с вопросом «купить» или «разрабатывать». Основные типы предоставления сервисов (Service Delivery Models) можно определить, как:

Insourcing

Insourcing – самостоятельная разработка, используя внутренние ресурсы организации на всех этапах жизненного цикла сервиса.

Преимущества:

- Прямой контроль
- Свобода выбора
- Быстрое создание прототипа и передовое обслуживание
- Удобные процессы и процедуры
- Применение специфики организации

Недостатки:

- Ограниченные ресурсы
- Может быть затратная в плане стоимости и времени выведения продукта на рынок
- Зависит от возможностей и уровня компетенции ресурсов организации

Outsourcing

Outsourcing – использование внешних ресурсов организаций, как полностью, так и частично на этапах жизненного цикла сервиса

Преимущества:

- Экономия масштаба
- Приобретение опыта и знаний
- Помогает организации сфокусироваться на основной деятельности
- Удобна при выполнении не системных задач
- Более формальный процесс тестирования новых продуктов

Недостатки:

- Меньший уровень непосредственного контроля
- Ограничения по выходу из проекта или изменению задач
- Риски, связанные с поставщиком продукта (платежеспособность, готовность продукта и т.п.)
- Неизвестность об уровне компетенции поставщика
- Более сложная модель организации
- Увеличивает долю проверки и соответствия продукта

Co-sourcing

Co-sourcing – комбинированное использование первых двух моделей

Преимущества:

- Снижает время выхода продукта на рынок
- Уверенность в уровне компетенции за счет выбора поставщика
- Высокий уровень контроля

Недостатки:

- Возможная сложность проекта
- Вопросы по защите интеллектуальной собственности
- Проблемы коммуникации в связи с различным уровнем культуры организаций

Partnership or Multi-sourcing

Partnership or Multi-sourcing – Формальное соглашение между организациями для совместной работы. Фокусируется на стратегическом партнерстве.

Преимущества:

- Снижает время выхода продукта на рынок
- Расширение рынка и выхода на него
- Взаимное получение выгоды

Недостатки:

- Сложность проекта
- Вопросы по защите интеллектуальной собственности
- Проблемы коммуникации в связи с различным уровнем культуры организаций

Business Process Outsourcing (BPO)

Business Process Outsourcing (BPO) – Формальное соглашение между организациями по частичному или полному переносу части бизнес функций.

Преимущества:

- Единая точка ответственности
- Передача риска
- Низкая стоимость передачи функций

Недостатки:

- Вопросы по защите интеллектуальной собственности
- Проблемы коммуникации в связи с различным уровнем культуры организаций
- Потеря бизнес знаний и связи с бизнесом по данному направлению

Application Service Provision (APO)

Application Service Provision – Формальное соглашение между организациями по использованию вычислительных ресурсов.

Преимущества:

- Доступ к производительным ресурсам
- Относительно низкая стоимость
- Использование по требованию

Недостатки:

- Вопросы по защите интеллектуальной собственности
- Проблемы коммуникации в связи с различным уровнем культуры организаций
- Потеря знаний по данному направлению

Knowledge Process Outsourcing (KPO)

Knowledge Process Outsourcing (KPO) – Формальное соглашение между организациями по полному переносу процессов и функций в аутсорсинг. Наблюдается при необходимости иметь высокий уровень качества, сервиса и экспертизы по данному направлению деятельности, а также снижение или перенос рисков.

Преимущества:

- Доступ к специализированным специалистам, знаниям и опыту
- Относительно низкая стоимость

Недостатки:

- Вопросы по защите интеллектуальной собственности
- Проблемы коммуникации в связи с различным уровнем культуры организаций
- Потеря знаний по данному направлению

Направления деятельности по управлению ИТ сервисами

Различают следующие два направления деятельности по управлению ИТ сервисами:

• *Предоставление сервиса (Service Delivery)*. Формирование ИТ сервиса и передача его к использованию.

• *Сопровождение сервиса (Service Support)*. Сопровождение ИТ сервиса в процессе эксплуатации.

Предоставления Сервиса (Service Delivery)

Основные цели Предоставления Сервиса (Service Delivery):

- Удовлетворение бизнес целей (Satisfy Business Objects)
- Эффективная разработка по стоимости и в срок (Be efficiently development in time scale & cost)
- Определение и управление рисками (Identify & Manage Risks)
- Дизайн методов и метрик (Design methods & metrics)
- Уменьшение Стоимости Владения (Total Cost of Ownership)
- Улучшение качества предоставления ИТ сервисов
- Улучшение ИТ сервисов
- Упрощение внедрения новых ИТ сервисов и изменения имеющихся
- Более эффективная работа ИТ сервисов
- Улучшение управления ИТ и соответствия бизнесу

Деятельность по Предоставлению Сервиса включает в себя следующие процессы:

- Управление Финансами
- Управление Мощностями
- Управление Непрерывностью
- Управление Доступностью
- Управление Уровнем Обслуживания

Основные аспекты по Предоставлению сервисов:

- Новые сервисы и изменение в существующих
- Инструменты и системы управление сервисами, портфель сервисов и сервисный каталог
- Технологическая архитектура и системы управления
- Следование процессам
- Методики и метрики измерений

Сфера ответственности направления предоставления сервисов – это цепочка: Люди – Процессы – Продукты – Поставщики.

Поддержка сервиса (Service Support)

Основные цели Поддержки Сервиса (Service Support):

- Поддержание заявленного уровня сервиса
- Восстановление нормального состояния сервиса после сбоя

Основные линии Поддержки Сервиса:

•Нулевая линия (L0) – регистрация инцидентов или самостоятельное устранение. В контексте данного документа подразумевает «нулевой» уровень ИТ знаний. Соответствует уровню знаний сотрудников организации или информационного центра. Предполагает самостоятельное решение инцидента на основе базы знаний.

•Первая линия (L1) – начальный уровень поддержки пользователей. В контексте данного документа подразумевает «базовый» уровень ИТ знаний. Соответствует уровню знаний техника департамента ИТ. Предполагает наличие базовых ИТ знаний и решение простых инцидентов на основе базы знаний.

•Вторая линия (L2) – специалисты по разрешению инцидентов данного типа или сервиса. В контексте данного документа подразумевает «продвинутый» уровень ИТ знаний. Соответствует уровню знаний специалиста департамента ИТ. Предполагает наличие углубленных ИТ знаний в определённой области. Является основным субъектом разрешения инцидентов.

•Третья линия (L3) – эксперты по разрешению инцидентов данного типа или сервиса. В контексте данного документа подразумевает «экспертный» уровень ИТ знаний. Соответствует уровню знаний эксперта департамента ИТ. Предполагает наличие как хороших теоретических знаний, так и достаточного опыта работы в определённой области. Максимальный уровень поддержки, при разрешении инцидентов.

•Четвертая линия (L4) – уровень поддержки со стороны производителя или профессионального сервиса. В контексте данного документа подразумевает поддержка на уровне производителя или поставщика продукта, или же специализированная организация. Обеспечивает максимальный уровень поддержки, как правило аутсорсинг, при разрешении инцидентов или проблем.

Деятельность по Поддержке Сервиса включает в себя следующие процессы:

- Управление Изменениями
- Управление Релизами
- Управление Проблемами
- Управление Инцидентами
- Управление Конфигурациями

Основные аспекты по Поддержке Сервисов:

- Формирование функции Поддержки Пользователей (Service Desk).
- Принцип организации «Единой точки контакта» (Single Point of Contact SPOC)

Управление непрерывностью ИТ сервисов

Процесс Управления Непрерывностью ИТ Сервисов является ключевым процессом по предоставлению ИТ услуг компаниям.

Управление непрерывностью ИТ сервисов управляет способностью услуг и их компонентов к восстановлению.

Стратегия обеспечения непрерывности должна включать в себя все рассмотренные ниже способы восстановления. Различные услуги, используемые организацией, требуют различных подходов к восстановлению и уменьшению рисков сбоя. Какая бы опция ни выбиралась, она должна быть экономически эффективной. Главное правило – чем дольше бизнес может обходиться без услуги, тем дешевле должно быть решение по обеспечению ее непрерывности. Показатели RPO, RTO, RLO, SDO напрямую связаны со стоимостью решений восстановления. Управление непрерывностью сервиса должно отображать реальные требования и возможности бизнеса. Управление непрерывностью ИТ сервисов (Pass 77: 2006) включает в себя процессы:

- BCM (Business Continuity Management)
- BCP (Business Continuity Planning)
- BCP (Business Contingency Planning)
- DRP (Disaster Recovery Planning)

- CEM (Crisis & Emergency Management)
- RA & RM (Risk Analysis & Risk Management)
- BEA (Business Environment Analysis)

Вводится понятие Уровень Непрерывности Бизнеса (Level of Business Continuity LBC).
Определены 7 уровней готовности к восстановлению:

- 0 – время не предсказуемо, или вероятность не восстановления
- 1 – резервное копирования на удаленных хранилищах
- 2 – резервное копирования на ленту или офлайн сайт
- 3 – Система Резервное Хранения Данных
- 4 – Point – in – time – copy
- 5 – целостность транзакций (актив/актив)
- 6 – нулевая потеря
- 7 – Автоматизация бизнеса

Кроме этого вводится классификация приложений и систем (ISO 17799:2002, NIST, COOP):

- Критически важные
- Критичные
- Существенные
- Не критичные

В дополнение к всему выше сказанному, необходимо наличие процесса Антикризисного управления.

Антикризисное управление (Crisis Management)

процесс, отвечающий за управление непрерывностью бизнеса в самом широком смысле. Команда антикризисного управления отвечает за стратегические вопросы, такие как управление взаимодействием со средствами массовой информации и доверием акционеров, а также принимает решение об инициации планов обеспечения непрерывности бизнеса.

В настоящее время технологии являются основным компонентом многих бизнес процессов, поэтому обеспечение их непрерывности и доступности является необходимым для существования бизнеса в целом.

Управление непрерывностью фокусируется на значимых негативных событиях, которые ИТIL называет «катастрофами» для бизнеса. Менее значимые события рассматриваются в рамках процесса Управления инцидентами. То, является ли какое-то конкретное событие катастрофой, зависит от организации, в которой оно произошло. Размер и значимость негативного влияния события на бизнес, например, финансовые потери или потеря репутации, измеряется в рамках Анализа влияния на бизнес. Анализ влияния на бизнес определяет минимальные требования к критичности, конкретные требования к технологиям и услугам определяются в рамках Управления непрерывностью.

ITSCM главным образом рассматривает активы ИТ и конфигурации, которые поддерживают бизнес-процессы. В случае катастрофы бизнесу необходимо перестроиться на альтернативную рабочую локацию. При этом необходимо предоставить такие элементы как удобство офиса для персонала, копии критических бумажных отчетов, услуги курьеров и телефонную связь для связи с клиентами и партнерами. В этой связи Управление непрерывностью должно учитывать количество и месторасположение офисов организации, а также услуги, предоставляемые в каждом из них.

Плана Реагирования Бизнеса на непредвиденные Обстоятельства (Business Contingency Plan)

План определяет порядок реагирования на непредвиденные обстоятельства для обеспечения непрерывности бизнеса, и его корреляция с действиями ИТ. Фокусируется на текущем состоянии сервисов и не катастрофических воздействий. В данный план входят требования по доступности сервиса, управление мощностями и т.п. Ключевые процессы при планировании непрерывности

бизнеса являются Управление инцидентами (IM), управление проблемами (PM), управление изменениями и релизами (CM).

В качестве важных показателей определяются следующие показатели:

- Точка Восстановления (Recovery Point Objective RPO)
- Время Восстановления (Recovery Time Objective RTO)
- Уровень Восстановления (Recovery Level Objective RLO)
- Уровень Состояния Сервиса (Service Delivery Objective SDO)
- Определение Среднего Времени Работы до Отказа (MTBF)
- Определение Среднего Времени Работы на Отказ (MTTF)
- Наработка на отказ (OTF)
- Определение Среднего Времени между Отказами (OTBF)
- Определение Среднего времени на восстановление сервиса (MTTR partly) до уровня «as usual»
- Определение Среднего времени на полное восстановление сервиса (MTTR full)
- MTPoD (Maximum Tolerable Period of Disruption)
- Maximum Acceptable Outage (MAO)
- Maximum Allowable Downtime (MAD)
- Maximum Tolerable Downtime (MTD)
- Mean Time to Detect (MTTD) проблемы, нарушения

Определение Плана Восстановления после катастроф (Disaster Recovery Plan)

План определяет порядок действий по восстановлению работоспособности бизнеса и его корреляция с действиями ИТ. Ключевые процессы при планировании плана восстановления являются управление инцидентами (IM), управление чрезвычайными ситуациями (СЕМ),

В качестве важных показателей определяются следующие показатели:

- Определение RPO, RTO, RLO и SDO
- Определение Среднего времени на восстановление сервиса (MTTR partly) до уровня «as usual»
- Определение Среднего времени на полное восстановление сервиса (MTTR full)

Плана Непрерывности Бизнеса (Business Continuity Plan)

Тоже самое что и План Реагирования на непредвиденные обстоятельства (Business Contingency Plan), но фокусируется на непрерывности и восстановлении работы после катастроф. Данный план определяет восстановление бизнеса после значительного ущерба в следствии воздействия катастроф. В отличие от План Реагирования Бизнеса на непредвиденные обстоятельства, план может включать в себя стратегические изменения в каталог ИТ сервисов.

План может включать в себя следующие планы управления непрерывностью:

План обеспечения непрерывности услуг (IT Service Continuity Plan) – план, определяющий шаги, необходимые для восстановления одной или нескольких услуг. План также должен определять события, которые являются основанием для его инициации, людей, которые должны быть задействованы, средства коммуникаций и т. п.

План обеспечения непрерывности бизнеса (Business Continuity Plan BCP) – план определяет шаги, необходимые для восстановления бизнес-процессов в случае нарушения их функционирования. План также должен содержать информацию о событиях, которые являются основанием для его инициирования; людях, которые должны быть задействованы в реализации плана; средствах коммуникаций и т. п.

Основные аспекты:

- Проведение BIA
- Определение превентивных мер
- Определение стратегии восстановления
- Определение плана Реагирования на воздействия
- Формирование команды по оценки ущерба
- Оценка ущерба
- Формирование команды по восстановлению
- Выполнение плана восстановления

Для формирования и выполнения плана может понадобиться наличие следующих команд:

- Команда по восстановлению (Restoration Team)
- Команда по оценке ущерба (Damage Assessment Team)
- Команда по спасению активов (Salvage Team)

Анализ сервисов и их влияние на бизнес (Business Impact Analysis BIA)

Анализ определяет порядок обеспечения непрерывности бизнеса, изменений в бизнес требованиях, а также действий ИТ. Деятельность в рамках процесса Управления непрерывностью бизнеса, которая определяет критичные бизнес-функции и их зависимость от факторов окружения. Этими факторами могут быть поставщики, люди, другие бизнес-процессы, услуги и т. д. BIA определяет последствия потери услуг для бизнеса. Потери могут быть значительными, например, крупные финансовые потери, и «мягкими» – моральные потери, потеря репутации, конкурентного преимущества и т. п.

Анализ влияния на бизнес определяет:

форму, которую может приобретать разрушение или потеря:

- потерянный доход;
- дополнительные затраты;
- вред репутации;
- потеря благосклонности клиентов;
- потеря конкурентного преимущества;
- повреждение и нарушение здоровья, законности и безопасности;
- риск безопасности персонала;
- потеря рынка сбыта в краткосрочном и долгосрочном периодах;
- потеря операционных возможностей, например, контроля.

как будут увеличиваться негативные последствия разрушения или потери после неблагоприятного события, а также время суток, недели, месяца, когда они будут наиболее серьезными;

кадровое обеспечение, навыки, аппаратура и услуги, которые необходимы для поддержки минимальных уровней непрерывности критичных бизнес-процессов;

временные рамки, в пределах которых необходимо обеспечить минимальный уровень восстановления кадрового обеспечения, аппаратуры, услуг и других возможностей;

временные рамки, в пределах которых необходимо полностью восстановить критичные бизнес-процессы и поддерживающие их кадровое обеспечение, аппаратуру, услуги и другие возможности;

приоритеты восстановления для услуг.

В качестве важных показателей определяются следующие показатели:

- Уровень влияния на целевую систему
- Уровень Состояния Сервиса (SDO)

Для визуального отображения может применяться таблица, с указанием сценариев отказа и результатов.

- Частичный отказ – Сервис продолжает работать благодаря 100% резервированию.
- Полный отказ – Полный отказ всей инфраструктуры.

Анализ сервисов и их влияние друг на друга (Service Failure Analysis SFA)

Анализ влияния на сервис со стороны других ИТ сервисов, изменений в бизнес требованиях, а также действий ИТ для обеспечения непрерывности бизнеса. Данный анализ позволяет определить критичность сервиса.

В качестве важных показателей определяются следующие показатели:

- Уровень влияния на целевую систему
- Уровень Состояния Сервиса (SDO)

Анализ может быть визуально отображается в виде двух таблиц:

- SFA (P) – зависимость работы сервиса от других сервисов и служб

- SFA (D) – зависимость других сервисов от отказа данного сервиса

Вспомогательные системы (F)	1	2	3	4	5	6	7	8	9
Корневые Сервисы (C)	1	2	3	4	5	6	7	8	9
Первичные Сервисы (P)	1	2	3	4	5	6	7	8	9
Вторичные Сервисы (S)	1	2	3	4	5	6	7	8	9
Вспомогательные Сервисы (A)	1	2	3	4	5	6	7	8	9
Бизнес Сервисы (B)	1	2	3	4	5	6	7	8	9
Сервисы защиты информации (D)	1	2	3	4	5	6	7	8	9

В качестве оценки может применяться качественный метод с указанием «веса» влияния (от 1 – полный отказ до 0 – не влияет)

1	Полный отказ
0.5	Частичный отказ
0	Не влияет
	Не определён
	Не применим

Анализ отказа компонентов сервиса (Components Failure Impact Analysis CFIA)

Анализ ИТ сервисов и влияние отказа его компонентов на работу сервиса. В качестве важных показателей определяются следующие показатели:

- Уровень отказа компонента системы
- Определение Среднего Времени Работы до Отказа (MTBF)
- Определение Среднего Времени Работы на Отказ (MTTF)
- Наработка на отказ (OTF)
- Определение Среднего Времени между Отказами (OTBF)

Визуально может отображен в виде таблицы компонентов, их важность, сценарии отказа и результат:

CFIA анализ – анализ работы сервиса при отказе компонентов сервиса

№	Компонент	Тип	1	2	3	4	5	6	7	8
1	OS Server 1	M	+	-	+	+	+	-	+	-
2	ADS Service Server1	M	+	-	+	-	+	-	-	-
3	OS Server 2	O	+	+	-	+	+	+	-	-
4	ADS Service Server2	O	+	+	-	+	-	-	-	-
	Результат		UP	UP	UP	UP	UP	DOWN	DOWN	DOWN

*- M-Обязательный, O-Опциональный компонент

При формировании политики Business Continuity & Disaster Recovery следует использовать дерево решений по следующим вопросам:

- Защита приложения
- Приоритет восстановления
- Выбор резервной площадки
- Связь между площадками
- Архитектура резервного копирования
- Архитектура хранения
- Архитектура репликации
- Архитектура инженерных систем
- Мониторинг производительности при переключении
- Тестирование DRP
- Утверждение факта катастрофы

Опции и методы восстановления

Опции восстановления в рамках Управление Непрерывностью Сервиса, которые должны быть учтены при формировании стратегии:

- переход на ручную работу
- взаимные соглашения
- постепенное восстановление (Gradual Recovery)
- промежуточное восстановление (Intermediate Recovery)
- быстрое восстановление (Fast Recovery)
- немедленное восстановление (Immediate recovery)

Переход на ручную работу для некоторых типов услуг может стать хорошей альтернативой на короткий период до восстановления услуги. Например, Сервис-деск может работать какое-то время с бумажными заявками и журналами;

Взаимные соглашения являются еще одной опцией для восстановления. Предполагают заключение соглашений между организациями, использующими похожие технологии. В настоящее время являются неприемлемыми для большинства ИТ-систем, но могут использоваться в отдельных случаях – например, для внешнего резервного копирования или использования принтеров;

Постепенное восстановление (Gradual Recovery) – способ восстановления, также известный как «холодное резервирование». Предусматривается восстановление услуги в течение более чем 72 часов. При постепенном восстановлении обычно задействован мобильный или стационарный резервный центр, оснащенный элементами жизнеобеспечения и сетевой разводкой, без компьютерных систем. Эта опция восстановления рекомендована для некритичных услуг, предоставление которых может быть задержано на дни и недели без значительного влияния на бизнес;

Промежуточное восстановление (Intermediate Recovery) – способ восстановления, также известный как «теплое резервирование». Предусматривается восстановление услуги в течение 24—72 часов. При промежуточном восстановлении обычно используется общий мобильный или стационарный резервный центр, оснащенный компьютерными системами и сетевыми компонентами. Конфигурирование аппаратного и программного обеспечения, а также восстановление данных выполняются в рамках Плана обеспечения непрерывности услуг. Данная опция восстановления обычно предлагается третьими сторонами, которые имеют для этого все необходимое оборудование и квалифицированный персонал. Стоимость этой опции восстановления зависит от ресурсов третьей стороны, которые должны быть задействованы для восстановления, а также от времени, в течение которого требуется восстановить услугу. Преимуществом данного метода является его прозрачность для пользователей. Недостатком – то, что информация (в том числе конфиденциальная) будет храниться у сторонней организации. Последнее делает неприемлемым данный способ восстановления для многих организаций.

Быстрое восстановление (Fast Recovery) – способ восстановления. Предусматривается восстановление услуги за короткий промежуток времени, обычно менее 24 часов. При быстром восстановлении обычно используется выделенный стационарный резервный центр с компьютерными системами и ПО, сконфигурированными для работы услуг. Немедленное восстановление может занимать до 24 часов, если требуется восстановление данных резервного копирования.

Немедленное восстановление (Immediate recovery) – способ восстановления, также известный как «горячее резервирование». Предусматривается восстановление услуги без прерывания услуги. Немедленное восстановление обычно использует технологии зеркалирования, балансировки загрузки и разделения площадок установки оборудования. Этот способ чаще всего предусматривает «двойную локацию» компонентов системы, то есть полное дублирование. Он является самым дорогим и применяется только для критичных бизнес-процессов, простой которых может оказать значительное негативное влияние на бизнес. Копии должны быть расположены на максимальном удалении от оригиналов, чтобы не быть задетыми разрушающим событием.

Перечень вопросов, регламентирующих ИТ процессы

Перечень вопросов, регламентирующих ИТ процессы и их описание.

- Назначение процесса – Определение процесса, отвечает на вопрос WHAT
- Цели процесса – Определяет цели и задачи процесса, отвечает на вопрос WHY
- Область применения – Определяет зону применения данного процесса, отвечает на вопрос WHEN.
- Зона ответственности – Определяет зоны ответственности для позиции или группы, отвечает на вопрос WHO.
- Процедуры- Процедуры, связанные с процессом, отвечает на вопрос HOW
- Критические Факторы Успеха (Critical Success Factors CSF) – Определяют, что должно произойти если процесс, сервис или проект будет успешным. Формируются критериями результативности (KGI).
- Критерии результативности (KGI) – Определяют критерии результативности достижения целей, не имеют явно выраженных измеряемых показателей. Формируются из показателей KPI и субъективных наблюдений контролирующего органа.
- Критерии эффективности (KPI) – Определяют критерии эффективности процессов, используемых для достижения целей. Формируются из метрик и показателей, которые можно измерить.
- Карта процесса – Описывает пошаговую цепочку действий.

№	Назначение процесса - (WHAT)	Цели процесса - (WHY)
1	Политики, процедуры по Управлению Требованиями.	Организация процесса Управления Требованиями, обсуждения, внесения изменений и принятие решения.
2	Порядок предоставления требований	Организация процесса предоставления требований
3	Порядок утверждения требований	Организация процесса утверждения требований
4	Контроль и мониторинг состояния	Организация контроля и мониторинга состояния

№	Процедуры - (HOW)	Зона ответственности - (WHO)			
		Responsible R	Authorized A	Involved C	Informed I
1.1	Предоставление требований со стороны бизнеса	дИТ	КИТ		
1.2	Анализ возможности	ИТ	дИТ		
1.3	Обсуждение и принятие решения	ИТ, Бизнес	КИТ		
1.4	Формирование пакета требований и уровня услуг	ИТ, Бизнес	КИТ		
1.5	Утверждение пакета требований и уровня услуг	ИТ, Бизнес	дИТ		
1.6	Контроль за исполнением	ИТ, Бизнес	дИТ		

№	Область применения - (WHEN)	Временные рамки (T)	Пред-процесс
1.1	Предоставление требований со стороны бизнеса	Не регламентируется	
1.2	Анализ возможности	+ 14 дней	1.1
1.3	Обсуждение и принятие решения	+ 14 дней	1.2
1.4	Формирование пакета требований и уровня услуг	+ 14 дней	1.3
1.5	Утверждение пакета требований и уровня услуг	+ 14 дней	1.4
1.6	Контроль за соблюдением	непрерывно	1.5

Критерии результативности - (KGI)

KGI Number	KGI Description	KPIs	Collected by	Reported to
DM		Demand Management		
KGI-DM-01	Удовлетворенность бизнеса			

Критерии эффективности - (KPI)

KPI Number	KPI Description	Good	Warning	Collected by	Reported to
DM		Demand Management			
KPI-DM-01	Количество заявленных требований к ИТ				
KPI-DM-02	Количество утвержденных требований	> 70%	< 70%		
KPI-DM-03	Количество отклоненных требований по причинам	< 30%			
KPI-DM-04	Количество требований связанных с изменениями				
KPI-DM-05	Количество требований связанных с проектами				
KPI-DM-06	Количество требований выполненных в срок	> 90%	< 90%		
	Полнота соответствия пакета требованиям бизнеса	> 70%	< 70%		

Матрица ролей и ответственностей (RACI Matrix)

Матрица ролей и ответственностей используется для определения ролей и ответственностей в процессе управления сервисами. Для каждой активности должна быть определена как минимум одна роль исполнителя и владельца. Базовая «стандартная» модель предполагает следующие роли:

RACI – стандартная модель

Responsible (R) – Исполнитель, может быть несколько на одну активность, может совмещаться

Accountable (A) – Несет ответственность, владелец. Может быть только один для задачи или действия.

Consulted (C) – Консультирует до исполнения

Informed (I) – Оповещается после исполнения

RASIC (RASCI) – модель

Responsible (R) – Исполнитель, может быть несколько на одну активность, может совмещаться

Accountable (A) – Несет ответственность, владелец. Может быть только один для задачи или действия.

Consulted (C) – Консультирует до исполнения

Informed (I) – Оповещается после исполнения

Supported (S) – Оказывает поддержку

RACI—VS (VARISC) – модель

Responsible (R) – Исполнитель, может быть несколько на одну активность, может совмещаться

Accountable (A) – Несет ответственность, владелец. Может быть только один для задачи или действия.

Consulted (C) – Консультирует до исполнения

Informed (I) – Оповещается после исполнения

Verifier (V) – Тот кто проверяет результаты

Signatory (S) – Тот кто подтверждает результаты проверки

RSI – модель

Responsible (R) – Исполнитель, может быть несколько на одну активность, может совмещаться

Sponsor (S) – Владелец, спонсор активности

Informed (I) – Оповещается после исполнения

DACI – модель

Driver (D) – Драйвер, принимает решения, может быть одна роль на проект.

Approver (A) – Подтверждает разрешает выполнение проекта или работ.

Contributor (C) – Специалисты, непосредственные исполнители (аналитики, разработчики и т п)

Informed (I) – Оповещается после исполнения

СТРАТЕГИЧЕСКИЙ ЭТАП (Strategy State)

Введение

Стратегический этап в управлении ИТ сервисами является по своей сути прикладным уровнем при построении ИТ Архитектуры Предприятия. Цели и задачи данного этапа:

- Показать организации как трансформировать Управление Сервисами в стратегические активы

- Внести ясность в связи между разными ИТ сервисами, системами или процессами и бизнес моделями и задачами

- Формирование стратегии сервиса, его цели и задачи.

- Определение ценность предоставляемых услуг и сервисов

- Определение возможностей ИТ по предоставлению сервисов

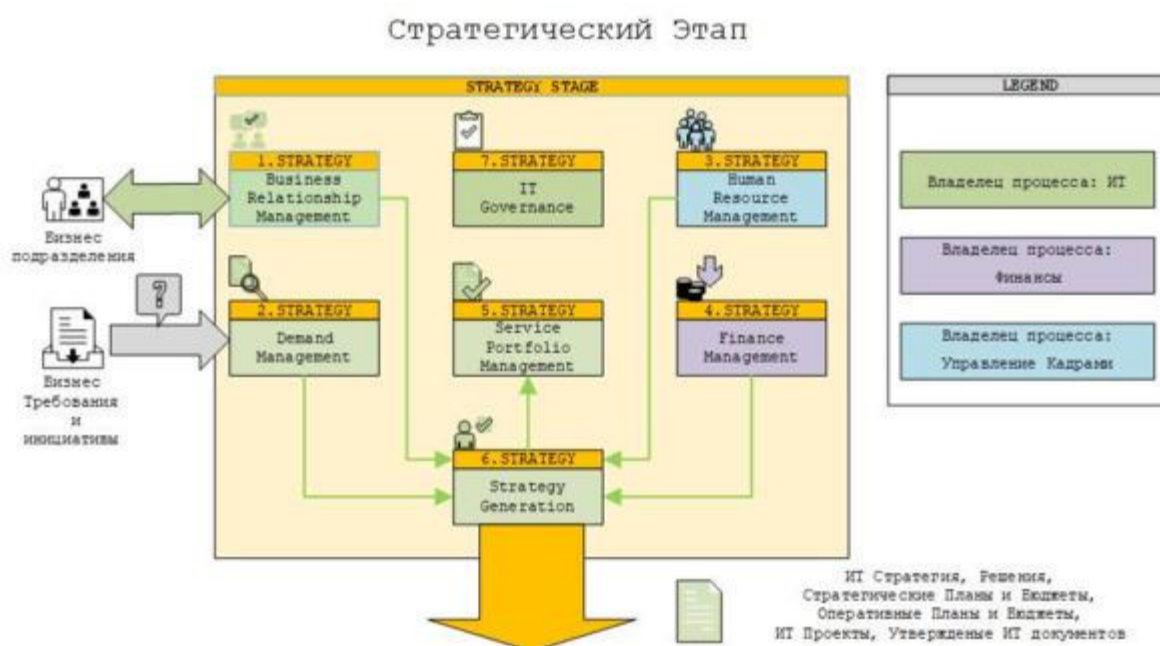
- Создание модели оказания услуг, охватывающие вопросы финансирования и внутреннюю организацию

Данный этап, по рекомендациям ITIL v3 определяется пятью процессами к которым я бы добавил еще два:

- Управление связями с бизнесом
- Управление требованиями (Demand management)
- Управление сотрудниками (HR Management) *
- Управление финансами (Financial management)
- Формирование Стратегии (Strategy Generation)
- Управление портфелем сервисов
- Управление Деятельностью ИТ (IT Governance) *

Процесс создания ценности для организации

Как важный элемент данного этапа необходимо определить ценность (Value) которое генерирует ИТ. Процесс создания ценности и связи запросов бизнеса с одной стороны, возможностей со стороны провайдера ИТ услуг (ИТ департамента), предоставляемых возможностей и стоимости.



Общий вид процессов показан на диаграмме. Рассмотрим процессы более подробно. На выходе стратегического этапа, руководство организации и ИТ директор имеет представление по направлению деятельности ИТ. Минимальный пакет документов представляет из себя ИТ Стратегию, Высокоуровневое описание ИТ Архитектуры Предприятия, Стратегические и Оперативные Планы ИТ, Стратегические и Оперативные Бюджеты ИТ, утвержденные решения по ИТ проектам. Разработанные и утвержденные документы по организации функционирования ИТ департамента.

Дополнительно, завершение стратегического этапа является решением к началу проекта, по методологии Управления Проектами соответствует фазе «инициализации» проекта. Как говорится «... ввяжемся в бой, а там посмотрим...».

Процессы стратегического этапа являются прикладными процессами при формировании ИТ Архитектуры Предприятия. Уже на данном этапе можно принять решения по тем или иным ИТ проектам. Например, бизнес сформулировал требования, по выполнению которых ИТ сможет предоставить решения, которые позволят бизнесу взлететь до небес (например, выращивать кукурузу на марсе, открыть филиал на луне или выпустить страховой продукт по страхованию летающих тарелок). Если данные предложения прошли на этапе анализа бизнес плана, что вполне возможно при достаточном уровне «компетенции» бизнеса. ИТ поможет «приземлить» бизнес, оценив приблизительную стоимость решения. Может получиться так, что требования

бизнеса достаточно приземленные и достижимы, но руководство организации сформулировало «... денег нет, но вы держитесь...». Тогда двигателем станет ИТ департамент, который имеющимися или минимальными ресурсами сможет покрыть лишь часть запроса. Бизнес должен будет выбрать подходит ли данный минимум или нет, и попыбует адаптироваться, изменить бизнес процессы, организацию и т п.

Управление Отношениями с Бизнесом (Business Relationship Management BR)

Процесс Управление Отношениями с Бизнесом предназначен для организации взаимодействия ИТ и бизнеса, и отвечает на такие вопросы как:

- Организация процесса взаимодействия ИТ с бизнесом
- Фокусирование внимания на бизнесе, их запросах и требованиях
- Анализ бизнес процессов, происходящих в бизнесе
- Оценка потенциала, по потребностям в услугах того или иного рода

Деятельность по процессу:

- Организация взаимодействия с бизнесом
- Разрешение конфликтов интересов

Входы процесса:

- Организационная структура компании
- Определение владельца сервиса

Выходы процесса:

- Определение сервиса
- Определение представителя бизнеса
- Определение управляющего ИТ сервисом
- Определение порядка информирования
- Протокол собрания

Участники процесса:

- Представители ИТ
- Представители бизнеса

Ключевые моменты процесса:

- Запросы со стороны бизнеса к ИТ могут носить неформальный характер на начальном этапе.
- Назначение представителей со стороны бизнеса и ИТ также может происходить в рамках рабочих процессов
- В качестве средств коммуникации может использоваться корпоративная почта, портал и т п.

Критерии результативности (KGI):

- Удовлетворенность бизнеса

Критерии эффективности (KPI):

- Количество запросов или инициатив от бизнеса
- Количество выполненных запросов (более 70%)
- Количество жалоб и недовольств (менее 10 за год)

Управление Требованиями (Demand Management DM)

Управление Требованиями один из основных процессов в функционировании ИТ любой организации и является ключевым для Стратегического этапа. Данный процесс отвечает на такие вопросы как:

- Понимание требований клиента к сервису на протяжении всего бизнес процесса.
- Гарантирование определённого уровня предоставления сервиса в соответствии с требованиями
- Гарантирования, что возможности и реализация (Utility & Warranty) сервиса удовлетворяют требованиям бизнеса.
- Сбор и обработка информации по работе ИТ сервиса
- Сбор и обработка запросов бизнеса
- Написание бизнес требований (BR)
- Контроль за соблюдением и выполнением требований

Деятельность по процессу:

- Формирование требований к ИТ сервисам
- Определение требований на основе активности (Activity-Based Demand Management)
- Определение Образцов и шаблона Бизнес Активности (Pattern of Business Activity PBA)
- Карта процессов
- Различия в бизнес циклах (день, неделя, месяц, квартал или год)
- Определение требований на основе бизнес ролей (User Profiles Demand Management)
- Функции и операции пользователей по процессам и приложениям
- Связывание роли с одним или более Образцами Бизнес Активности (PBA)
- Формирование Core Services Packages и Supporting Services
- Формирование Service Level Packages
- Объединение SLP и CSP для формирования Каталога Сервиса
- Разработка пакетов предоставления сервисов

При определении бизнес требований можно использовать MoSCoW анализ:

M – Должно быть

S – Следует иметь если это возможно

C – Можем иметь, но без воздействия на что-то другое

W – Не нужно сейчас, но может понадобится в будущем

Входы процесса:

Стратегический и оперативные планы организации

Требования со стороны бизнеса

Требования со стороны бизнеса

Шаблоны Активности Бизнеса (Patterns of Business Activity)

Пользовательские активы

Ожидания бизнеса

Ограничения

Выходы процесса:

Пакет Сформулированных Требований к ИТ сервису (Core Service Packages) включая технические и бизнес сервисы

Пакет Сформулированных Требований к уровню оказания услуг по сервису (Service Level Packages)

Соглашение об Уровне Услуг

Требования к ресурсам

Требования к финансам

Участники процесса:

Представители бизнеса

Представители ИТ

Ключевые моменты процесса:

Требования должны быть документально зафиксированы и подтверждены.

Уровень подтверждения зависит от требований организации (руководитель бизнес подразделения, руководство организации и т.п.)

ИТ департамент является владельцем процесса.

№	Назначение процесса - (WHAT)	Цели процесса - (WHY)
1	Политики, процедуры по Управлению Требованиями.	Организация процесса Управления Требованиями, обсуждения, внесения изменений и принятие решения.
2	Порядок предоставления требований	Организация процесса предоставления требований
3	Порядок утверждения требований	Организация процесса утверждения требований
4	Контроль и мониторинг состояния	Организация контроля и мониторинга состояния

№	Процедуры - (HOW)	Зона ответственности - (WHO)			
		Responsible R	Authorized A	Involved C	Informed I
1.1	Предоставление требований со стороны бизнеса	ИТ	КИТ		
1.2	Анализ возможности	ИТ	КИТ		
1.3	Обсуждение и принятие решения	ИТ, Бизнес	КИТ		
1.4	Формирование пакета требований и уровня услуг	ИТ, Бизнес	КИТ		
1.5	Утверждение пакета требований и уровня услуг	ИТ, Бизнес	КИТ		
1.6	Контроль за исполнением	ИТ, Бизнес	КИТ		

№	Область применения –(WHEN)	Временные рамки (T)	Пред-процесс
1.1	Предоставление требований со стороны бизнеса	Не регламентируется	
1.2	Анализ возможности	+ 14 дней	1.1
1.3	Обсуждение и принятие решения	+ 14 дней	1.2
1.4	Формирование пакета требований и уровня услуг	+ 14 дней	1.3
1.5	Утверждение пакета требований и уровня услуг	+ 14 дней	1.4
1.6	Контроль за соблюдением	непрерывно	1.5

KPI Number	KPI Description	Good	Warning	Collected by	Reported to
DM	Demand Management				
KPI-DM-01	Количество заявленных требований к ИТ				
KPI-DM-02	Количество утвержденных требований	> 70%	< 70%		
KPI-DM-03	Количество отклоненных требований по причинам	< 30%			
KPI-DM-04	Количество требований связанных с изменениями				
KPI-DM-05	Количество требований связанных с проектами				
KPI-DM-06	Количество требований выполненных в срок	> 90%	< 90%		
	Полнота соответствия пакета требованиям бизнеса	> 70%	< 70%		

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Управление Сотрудниками (HR Management HR)

Процесс Управление Сотрудниками, отвечает на такие вопросы как:

Стратегическое и тактическое планирование ИТ ресурсов (сотрудников)

Управление персоналом должно способствовать достижению стратегических целей организации

Создание работникам условий, для применения и развития своих способностей для целей организации

Набор сотрудников в ИТ департамент

Продвижение и повышение сотрудников

Определение должностных инструкций

Деятельность по процессу:

Формирование процесса управления сотрудниками

Формирование процесса непрерывного обучения и роста сотрудников

Формирование процесса мотивации сотрудников

Формирование благоприятного климата в организации

Определение процедуры регистрации нового сотрудника

Определение процедуры регистрации изменения атрибутов сотрудника

Определение процедуры регистрации ухода сотрудника

Назначение процесса (WHAT) и цели процесса (WHY):

Организация процесса управления сотрудниками

Управление сотрудниками

Формирование должностных инструкций сотрудников ИТ

Формирование позиций и градаций в ИТ департаменте

Набор сотрудников в ИТ департамент

Тестирование и собеседования

Обучение сотрудников организации

Обучение сотрудников ИТ департамента
Оценка и аттестация сотрудников ИТ департамента
Мотивация сотрудников ИТ департамента

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

Разработка процесса управления сотрудниками
Утверждение процесса управления сотрудниками
Внесение изменений в процесс управления сотрудниками
Регистрация нового сотрудника
Организация рабочего места сотрудника
Предоставление доступа сотруднику
Регистрация изменений по сотруднику
Изменений рабочего места сотрудника
Изменений доступов сотруднику
Убытие сотрудника
Сворачивание рабочего места сотрудника
Закрытие доступа сотруднику
Разработка должностных инструкций сотрудника
Согласование должностных инструкций сотрудника
Утверждение должностных инструкций сотрудника
Внесение изменений в должностные инструкции сотрудника
Разработка позиций и градаций сотрудника
Согласование позиций и градаций сотрудника
Утверждение позиций и градаций сотрудника
Внесение изменений в позиции и градации сотрудника
Планирование кадровых ресурсов
Формирование требований к сотрудникам
Подготовка ИТ тестов
Проведение собеседования
Самостоятельное обучение сотрудника
Проведение обучения внутри компании (общие вопросы)
Проведение обучения внутри компании (технические вопросы)
Проведение обучения на курсах
Самостоятельное обучение сотрудника
Проведение обучения внутри компании (общие вопросы)
Проведение обучения внутри компании (технические вопросы)
Проведение обучения на курсах
Оценка и аттестация сотрудников ИТ департамента
Подготовка тестов для аттестации ИТ сотрудника
Проведение тестирования ИТ сотрудника
Проведение аттестации ИТ сотрудника
Оценка результатов ИТ сотрудника
Мотивация сотрудников ИТ департамента
Премирование ИТ сотрудника
Продвижение ИТ сотрудника
Повышение ИТ сотрудника

Входы процесса:

Политики и процедуры со стороны Департамента Отдела Кадров
Организационная структура ИТ департамента
ИТ стратегия и планы организации
ИТ стратегия
ИТ проекты
Процесс Управления Знаниями

Участники процесса:

ИТ комитет

Отдел Кадров

Выходы процесса:

Протокол решения ИТ комитета

Организация ИТ департамента

Планирование человеческих ресурсов

Ключевые моменты процесса:

Департамент Управления Кадрами является владельцем и управляющим процессом

ИТ департамент выполняет требования владельца процесса

Критерии результативности (KGI):

Удовлетворенность бизнеса

Критерии эффективности – (KPI)

Количество часов обучения для сотрудников

Количество часов внутреннего обучения

Количество часов обучения по сотрудникам

Срок пребывания сотрудника на должности

Средний бал набранный при тестировании или аттестации

Стоимость обучения по сотрудникам

Среднее время между обучением и получения достаточного уровня компетенции

Знания сотрудника по отношению к имеющимся сервисам

Стоимость внешнего обучения сотрудника

Стоимость внутреннего обучения сотрудника

Соответствие фактических задач сотрудника и должностных инструкций

Показатели ротации и взаимозаменяемости сотрудников

Управление Финансами (Finance Management FM)

Управление Финансами является ключевым процессом в функционировании ИТ любой компании. Управление финансами отвечает на такие вопросы как:

Финансовая прозрачность и возможность учета

Контроль за финансовой активностью

Управление стратегическими инвестициями

Понимание стоимости предоставляемых услуг (Total Cost of Ownership TCO)

Понимание ценности полученных клиентов от использования сервисов

Улучшает процесс принятия решений на всем жизненном цикле сервиса.

Предоставление финансовой отчетности

Деятельность по процессу:

Разработка и утверждение Стратегического Бюджета ИТ

Разработка и утверждение Оперативного Бюджета ИТ

Контроль за финансами (закупки)

Контроль за финансами (текущие и плановые расходы)

Контроль за зарплатой, премиями и т.п.

Оценка стоимости сервиса

Оценка потерь из-за простоя сервиса

Оптимизация стоимости сервисов

Моделирование переменных затрат

Разработка модели финансирования

Разработка модели анализа и анализ ROI, IRR, бизнес кейсов

Разработка модели инвестиций в ИТ

Формирование и согласование с финансовым департаментом центров расходов

Разработка модели рефинансирования

Назначение процесса (WHAT) и цели процесса (WHY):

формирования стратегического ИТ

формирования оперативного ИТ бюджета

Внесение изменений в ИТ бюджет

Контроль ИТ бюджета контроль стратегического и оперативного ИТ бюджета

Контроль расходов ИТ контроль оперативных расходов

Контроль расходов по ИТ проектам контроль бюджета по ИТ проектам

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

Предоставление ИТ стратегии

Формирование стратегического ИТ бюджета

Обсуждение стратегического ИТ бюджета

Принятие стратегического ИТ бюджета

Ознакомление со стратегическим ИТ бюджетом

Контроль за исполнением стратегического ИТ бюджета

Предоставление ИТ стратегии

Формирование оперативного ИТ бюджета

Обсуждение оперативного ИТ бюджета

Принятие оперативного ИТ бюджета

Ознакомление с оперативным ИТ бюджетом

Контроль за исполнением оперативного ИТ бюджета

Предоставление изменений

Анализ изменений

Обсуждение изменений ИТ бюджета

Принятие изменений

Ознакомление с изменениями

Внесение изменений в ИТ бюджет

Формирование ежемесячного отчета

Предоставление ежемесячного отчета

Сверка ежемесячного отчета

Подтверждение ежемесячного отчета

Счет предоставляется в ИТ департамент

Регистрация передачи документа

Подтверждается факт выполнения работ

Документ визируется на оплату

Регистрация передачи документа

Передача документа в финансовый департамент

Регистрация передачи документа

Входы процесса:

Стратегические и оперативные планы ИТ

Требования бизнеса

Портфель сервисов

Каталог сервисов

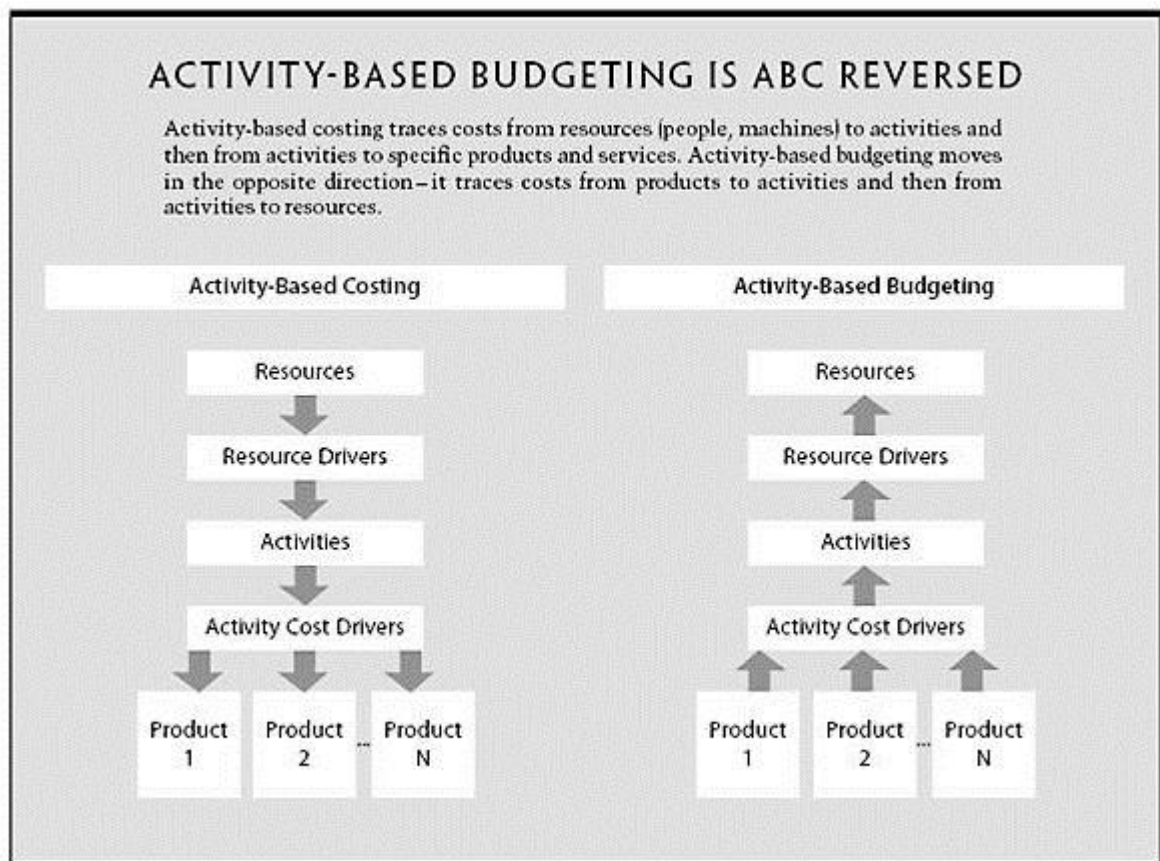
Выходы процесса:

Подписанный протокол решения ИТ комитета

Подписанный Стратегического Бюджета ИТ

Подписанный Оперативного Бюджета ИТ

Предоставление финансовой отчетности



Участники процесса:

ИТ Комитет.

Финансовый директор

ИТ директор

Ключевые моменты процесса:

Комитет ИТ собирается не реже чем один раз в квартал

Условия проведения ИТ комитета (Наличие кворума)

Порядок распределения «веса» голосов при голосовании («А» роль)

Порядок принятия решения (простое большинство, кворум, полное согласие или «последнее слово» владельца)

ИТ директор не имеет права «голосовать», а выполняет рекомендательную функцию («С» роль)

Возможность совмещение проведения комитетов по SG и FM

Финансовый департамент является владельцем процесса

ИТ департамент обеспечивает управление процессов, если имеется соответствующие ИТ компоненты

Требования по Управлению Финансами определяется со стороны департамента Финансов и бухгалтерии

Критерии результативности – (KGI):

Соответствие ИТ бюджета ИТ стратегии

Удовлетворённость владельцев бизнеса

Критерии эффективности – (KPI)

Соответствие ИТ бюджета

Соответствие расходов утвержденному ИТ бюджету

Количество изменений, внесенных в ИТ бюджет

Стоимость процесса управления ИТ

Стоимость сопровождения ИТ инфраструктур

Полная стоимость владения ИТ инфраструктурой

Стоимость резервной площадки

Стоимость ИТ сервисов и ИТ активов

Стоимость ИТ сервисов на пользователя

Стоимость «операционной» ИТ среды (Production)

Стоимость «тестовой» ИТ среды (Test)

Стоимость «эталонной» ИТ среды (Pre-production)

Соотношение стоимости Бизнес и Технических ИТ сервисов

Соотношение стоимости основной и резервной площадки

Стоимость ИТ проектов

Административные расходы ИТ департамента

Стоимость персонала ИТ департамента

Соотношение основного и вспомогательного персонала ИТ

Разработка Стратегии (Strategy Generation SG)

Разработка стратегии является ключевым процессом в функционировании ИТ любой компании и является основным для стратегического этапа. Выходы процессов стратегического этапа являются входными данными для процесса разработки стратегии. Процесс отвечает на такие вопросы как:

Стратегия ИТ департамента

Соответствие ИТ стратегии и стратегии бизнеса

Какие сервисы и кому необходимо предоставлять

Как создавать ценность для клиента или бизнеса

Как разрешать конфликты требований к разделяемым ИТ ресурсам

Разработка стратегических активов

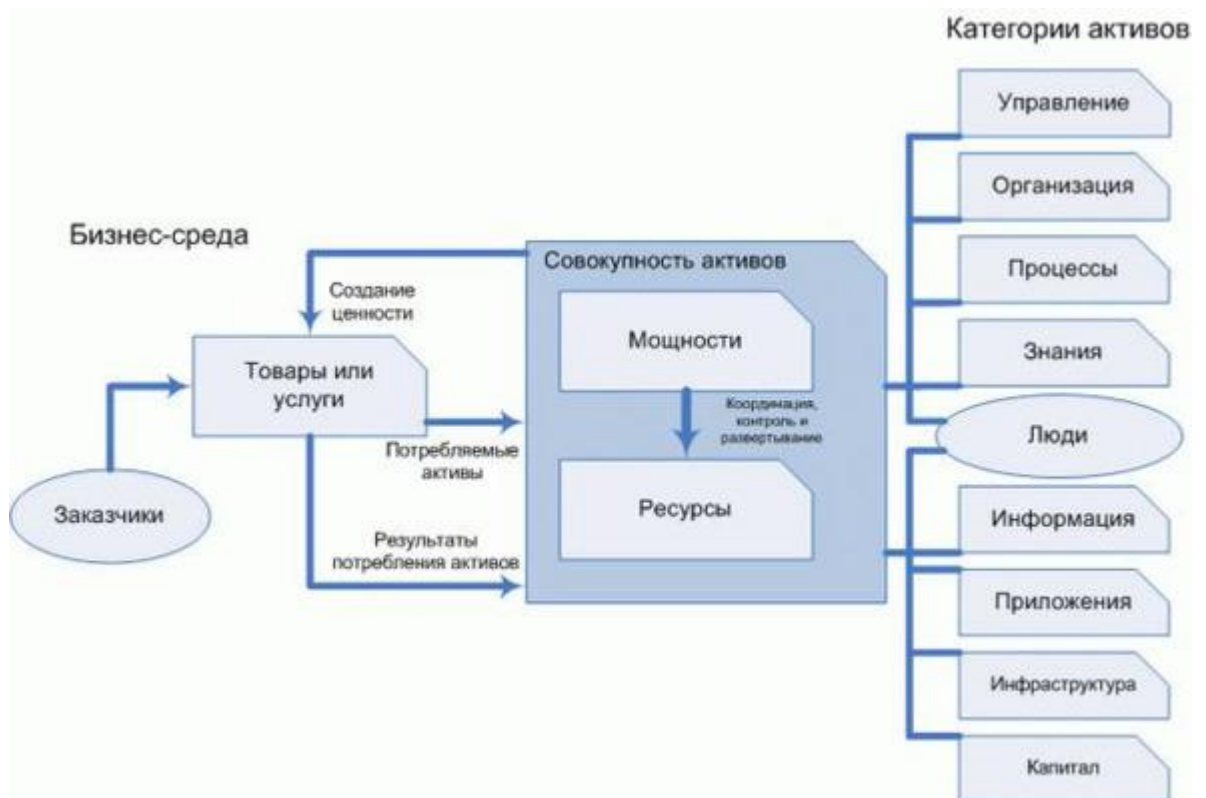
Оценка сильных и слабых сторон, приоритеты и риски

Как распределять ресурсы и мощности между сервисами портфеля

Понимание рынка и идентификация возможностей по созданию сервисов

Разработка outcome-based service, которые предоставляют функциональность заказчикам

Подготовка и удачная реализация стратегии



Деятельность по процессу:

- Разработка и утверждение Плана Стратегического Развития ИТ
- Разработка и утверждение Оперативного Плана Развития ИТ
- Контроль за исполнением планов ИТ
- Разработка и утверждение руководящей документации
- Разработка системы контроля (Develop closed-loop control system)
- Разработка стратегических активов и сервисов
- Анализ мощностей и ресурсов
- Анализ стратегии и сервисов
- Понимание нужд заказчика
- Понимание возможностей
- Классификация и визуализация сервисов как образцов создания ценности
- Определение outcome-based service
- Разработка портфеля сервисов
- Оценка стратегии
- Постановка целей и задач
- Соответствие активов и нужд заказчиков
- Определение критических факторов успеха
- Определение приоритетов инвестиций
- Исследование бизнес потенциала
- Asset-based services
- Utility-based services
- Планы и Patterns
- Создание ценности
- Определение сильных и слабых сторон
- Определение возможностей и угроз
- Необходимые компетенция

Входы процесса:

План стратегического развития организации
Организационная структура компании
Бизнес требования
Портфель сервисов
Каталог сервисов
Оценка рисков
Стоимость сервисов
Определение Стратегии Обслуживания (Lines of Service)
Шаблоны бизнес процессов и активности
Оценка мощностей
Оценка ресурсов
Оценка ограничений
Оценка конфликтов
Стратегический анализ
Определения рынка
Ограничения заказчика
Выгоды
Бизнес задачи



Выходы процесса:

Подписанный протокол решения ИТ комитета
Утвержденная ИТ Стратегия
Подписанный Плана Стратегического Развития ИТ
Подписанный Плана Оперативного Развития ИТ
Подписанные Проекты
Подписанные руководящие документы ИТ

Решения по инвестициям

Участники процесса:

ИТ Комитет

Менеджер по взаимодействию с бизнесом

Директор ИТ департамента

Представители бизнеса

Ключевые моменты процесса:

Принятие стратегических решений должно проходить этап утверждения со стороны руководства организации.

ИТ комитет является высшим органом по принятию решений в области ИТ

ИТ Комитет собирается не реже чем один раз в квартал.

Наличие кворума для принятия решения (рекомендации со стороны Юридического департамента)

Порядок распределения «веса» голосов при голосовании («А» роль)

Порядок принятия решения (простое большинство, кворум, полное согласие или «последнее слово» владельца)

ИТ директор не имеет права «голосовать», а выполняет рекомендательную функцию («С» роль)

Назначение процесса (WHAT) и цели процесса (WHY):

Формирования процесса управления ИТ стратегии

Внесение изменений в ИТ стратегию

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

Предоставление бизнес стратегии

Формирование ИТ стратегии

Обсуждение ИТ стратегии

Принятие ИТ стратегии

Ознакомление с ИТ стратегией

Исполнение ИТ стратегии

Контроль выполнения ИТ стратегии

Предоставление изменений

Анализ изменений

Обсуждение изменений ИТ стратегии

Принятие изменений

Ознакомление с изменениями

Внесение изменений в ИТ стратегию

Критерии результативности – (KGI)

Соответствие ИТ стратегии бизнес стратегии

Удовлетворённость владельцев бизнеса

Критерии эффективности – (KPI)

Исполнимость стратегических планов в срок > 70%

Исполнимость оперативных планов в срок > 70%

Количество изменений, внесенных в ИТ стратегию

Управление Портфелем Сервисов (Service Portfolio Management PM)

Процесс Управление Портфелем Сервисов рассматривает ИТ сервисы с точки зрения бизнес ценности для организации. Его можно рассматривать как динамический метод управления инвестициями в управлении ИТ услугами на уровне организации.

Цели процесса:

Перечень сервисов, имеющихся в ИТ департаменте на всех стадиях жизненного цикла (в разработке, внедрении, сопровождении, выведенных из эксплуатации и т.п.).

Перечень сервисов (бизнес услуг), предоставляемых клиентам

Почему клиент использует данный сервис

Почему клиент должен использовать сервис, предоставляемый нами, платить за него

Почему именно у нас клиент покупает данный сервис

Какова модель финансирования сервиса

Каковы сильные и слабые стороны, приоритеты и риски

Как распределять ресурсы и мощности между сервисами портфеля

Деятельность по процессу:

Формирование портфеля сервисов

Разработка мощностей и ресурсов

Входы процесса:

Выходные данные Стратегии

Выходы процесса:

Inventories

Business Cases

Service Portfolio

Authorization

Value Proposition

Prioritization

Communication

Resource Allocation

Участники процесса:

ИТ комитет

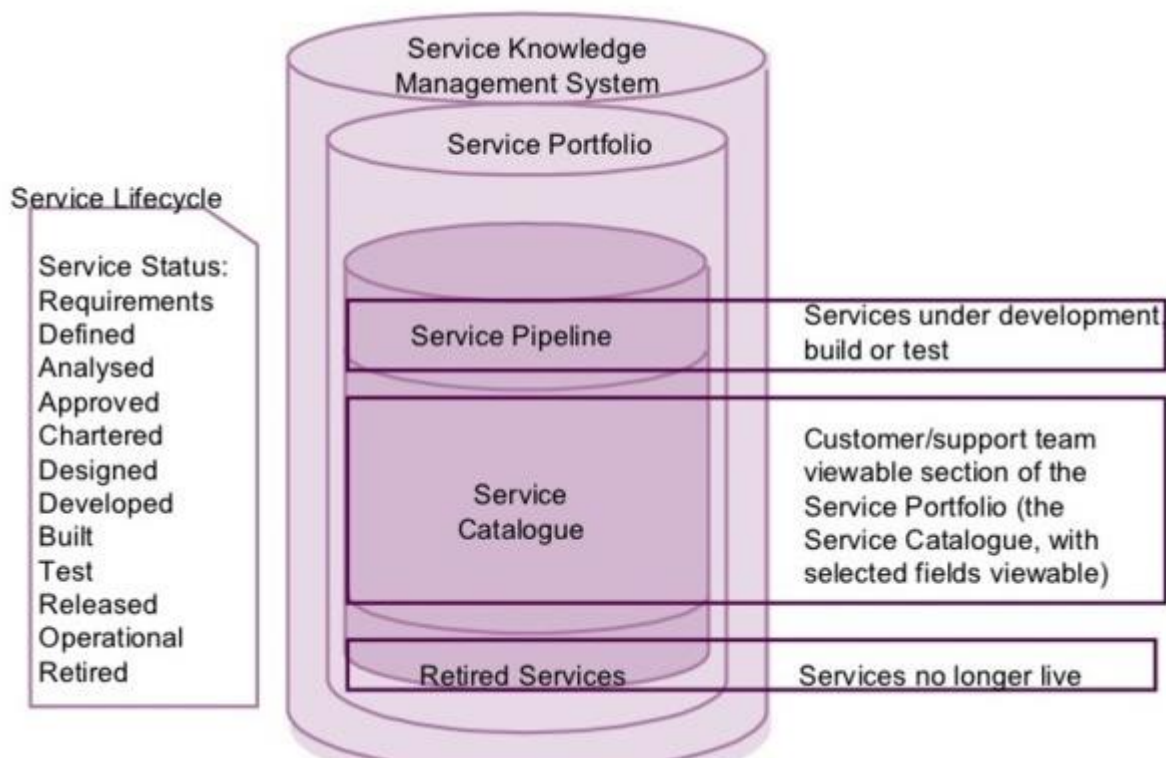
Contract Manager

Business Relationship Manager

Product Manager

Ключевые моменты процесса:

Владелец процесса является ИТ



Определены следующие статусы сервисов:

Требования (Requirements) – набор требований, полученных от бизнеса или ИТ департамента

Установленные (Defined) – набор требований, которые были определены, оценены и задокументированы и Уровень Требования к Сервису (SLR) сгенерированы

Проанализированы (Analysed) – набор требований, который был проанализирован и установлены приоритеты

Одобрены (Approved) – набор требований, которые были утверждены и задокументированы

Заказанные (Chartered) – сервисы, для которых выделены ресурсы и бюджет

Проектированы (Designed) – сервис или его компоненты, спроектированы и при необходимости закуплены

Разработаны (Developed) – сервис или его компоненты, разработаны

Собранные (Built) – сервис или его компоненты, собраны

Протестированные (Tested) – сервис или его компоненты, прошедшие тестирование

Выпущенные (Released) – сервис или его компоненты, сборка которого готова

Сопровождается (Operational) – сервис или его компоненты, предоставленные клиентам и сопровождаются

Устаревшие (Retired) – сервис или его компоненты, выведенные из «производственной» среды

Различные элементы одной услуги могут иметь различные статусы в один момент времени. Каждая организация должна аккуратно проектировать Портфель услуг, его содержание и доступ к нему. Содержание Портфеля услуг должно включать в себя следующую информацию:

Имя услуги

Описание услуги

Статус услуги

Классификацию услуги и ее критичность

Используемые приложения

Используемые данные или/и схемы данных

Бизнес-процессы, поддерживаемые услугой
 Владельцы бизнеса
 Пользователи бизнеса
 Владельцы ИТ
 Уровень гарантии качества услуги, ссылки на SLA и SLR
 Поддерживающие услуги
 Поддерживающие ресурсы
 Услуги, которые зависят от рассматриваемой услуги
 OLA, контракты и соглашения
 Затраты на услугу
 Издержки на услугу (если это применимо в данном случае)
 Доход от услуги (если это применимо в данном случае)
 Метрики для услуги

Поле	Значение (пример)	Описание
ID	C01	Уникальный Идентификатор сервиса
Service Group	Technical	Группа сервисов
Service Name	Platform of Virtualization	Наименование сервиса
Service Description	Предоставляет вычислительные мощности (CPU, RAM) для работы виртуальных машин	Краткое описание назначения сервиса
Service Status	Active	Статус сервиса
Vendor	Microsoft	Производитель используемый в сервисе
Supplier	ABC MMC	Сторонний поставщик (продавец) сервиса
Supplier Contacts	Name Surname, e-mail, phone etc	Контактная информация по поставщику сервиса
Severity	Critical	Приоритет сервиса
Service Owner	IT Department	Владелец сервиса (бизнес)
Service Manager	Name Surname, Infrastructure Division	Управляющий сервисом (руководитель ИТ подразделения ответственный за сопровождение сервиса)
Started in production	01.01.2017	Дата запуска сервиса в работу
Vendor Support	Basic technical support 24/7 with 8 hours response	Уровень поддержки со стороны производителя, статус
Supplier Support	Advanced technical support 24/7 with 2 hours response	Уровень поддержки со стороны поставщика, статус
Escalation Workflow	L1/L2/L3 according to Incident Management Procedure XXX	Процесс эскалации инцидента, запроса или проблемы по сопровождению сервиса (в пределах организации)
L4 Escalation Workflow	Only L3 according to Incident Management Procedure XXX	Процесс эскалации инцидента, запроса или проблемы по сопровождению сервиса (на уровень производителя или поставщика). Имеет значение если уровень поддержки L4 имеет дополнительную стоимость.
Service Components	HOST01, HOST02, HOST03, C02, etc	Элементарные компоненты инфраструктуры, входящие в состав сервиса.

Пример содержания каталога сервисов (включает, но не ограничивает):

Портфель сервисов позволяет уже на этапе стратегического планирования иметь перечень сервисов, которые ИТ департамент планирует предоставлять, отслеживать изменение статуса сервиса, инициатора, время, прошедшее от утверждения решения до внедрения сервиса.

Критерии результативности – (KGI)
 Полнота и достоверность портфеля
 Быстрота внедрения в каталог сервисов

Критерии эффективности – (KPI)
 Количество сервисов в портфеле
 Количество сервисов по статусам
 Количество сервисов по типам (Б/Т)
 Количество сервисов по бизнес подразделениям

Время перехода в каталог сервисов
Время перехода из каталога сервисов
Своевременность и полнота информации
Несвоевременная регистрация
Отношение сервисов каталога к сервисам портфеля

Управление деятельностью ИТ департамента (IT Governance DG)

Процесс управления деятельностью ИТ департамента является вспомогательным процессом в функционировании ИТ. В контексте управления ИТ сервисами рассматривается не как стандарты по Управлению ИТ, а вспомогательный процесс, регулирующий деятельность по принятию решений, организацию работы с руководящими документами ИТ и т.п. Управление ИТ отвечает на такие вопросы как:

Регламентирование административных мероприятий по управлению ИТ
Организация работы с ИТ документацией по управлению ИТ сервисами

Деятельность по процессу:

Разработка и утверждение процессов управления и взаимодействия ИТ
Разработка и утверждение руководящих ИТ документов
Разрешение конфликта интересов

Входы процесса:

Требования бизнеса
Рекомендации мировых практик в области управления ИТ, Управления Проектами, Аудита, Корпоративного Управления

Выходы процесса:

Протокол решений ИТ комитета и Руководящие ИТ документы

Участники процесса:

ИТ Комитет

Ключевые моменты процесса:

Комитет ИТ собирается не реже чем один раз в квартал

Владельцем процесса является ИТ департамент. При высоком уровне зрелости организации, владельцем процесса может быть административный департамент, в рамках корпоративного управления организацией в целом.

ИТ департамент обеспечивает управление процессов, если имеются соответствующие ИТ компоненты

Назначение процесса (WHAT) и цели процесса (WHY):

Организация процесса управления ИТ формирования стратегического ИТ бюджета
Организация деятельности ИТ формирования оперативного ИТ бюджета

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

Формирование руководящих документов ИТ
Обсуждение руководящих документов ИТ
Принятие руководящих документов ИТ
Регистрация решения ИТ комитета
Сбор подписей по решению ИТ комитета
Регистрация документов в отделе документооборота
Ознакомление с руководящими документами ИТ
Контроль за исполнением руководящих документов ИТ
Внесение изменений в руководящие документы ИТ
Разрешение конфликтов интересов

Критерии результативности – (KGI)
Удовлетворённость владельцев бизнеса

Критерии эффективности – (KPI)
Количество утвержденных руководящих ИТ документов
Количество внесенных изменений в руководящие ИТ документы
Количество и сроки проведения ИТ комитетов
Нарушения по количеству или срокам проведения ИТ комитетов

ЭТАП ДИЗАЙНА (Design Stage)

Введение

Этап Дизайна является не менее важным и наиболее объемным этапом управления ИТ сервисами. На данном этапе производится планирование сервиса, детализация всех аспектов функционирования сервиса, закладывается основа плана внедрения и сопровождения сервиса. По сути происходит основная «мозговая» деятельность. Для Управления Проектами соответствует фазе планирования проекта.

Цели и задачи:

Проектирование новых и изменение имеющихся сервисов для организации

Сервис дизайн вовлекается только для «важных» стратегических изменений в ИТ архитектуре.

Формирование дизайна и планирование сервиса и процессов.

Данный этап определяется следующими процессами (7):

Координация дизайна и планирования (Design Coordination) *

Управление рисками (Risk Management) *

Управление архитектурой (Architecture Management) *

Управление соответствия требованиям (Compliance Management) *

Управление Каталогом Сервисов (Service Catalogue Management)

Управление Уровнем Услуг (Service Level Management)

Управление доступностью (Availability Management)

Управление мощностями (Capacity Management)

Управление непрерывностью сервисов (It service Continuity Management)

Управление Информационной Безопасностью (Information Security Management)

Управление поставщиками (Supplier Management)

Деятельность процессов дизайна концентрирует свое внимание на двух ключевых аспектах:

Ресурсы (Resources) – прямые активы которые можно измерить

Возможности (Capability) – способности организации координировать, контролировать и распределять ресурсы для создания ценности.

Помимо этого, вводятся два важных атрибута сервиса:

Возможности сервиса (Utility), что он делает. Соответствие функциональным требованиям «fit to purpose».

Качество сервиса (Warranty) – насколько хорошо он это делает, «fit for use».

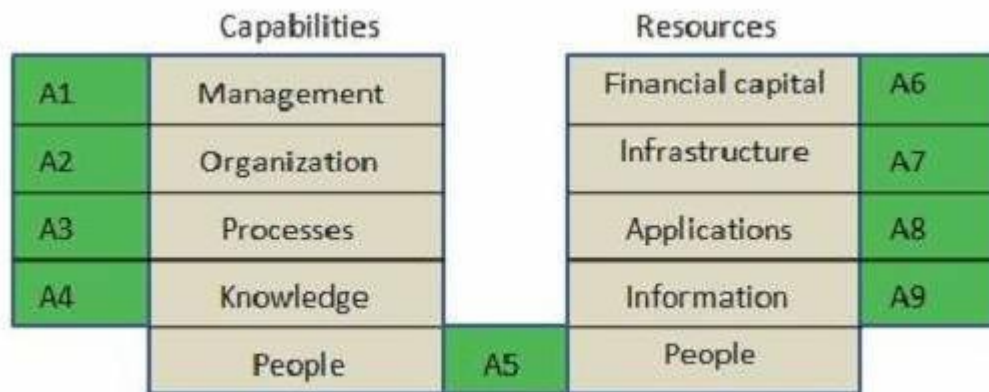
Этап Дизайна сервисов оперирует четырьмя основными понятиями:

Люди (People)

Продукты (Products)

Процессы (Processes)

Партнеры (Partners)



Основные измерения этапа Дизайна сервисов:

Функциональность (возможности сервиса)

Ресурсы (люди, финансы, технологии)

Время

Баланс этих трех показателей позволяет достичь максимальной эффективности этапа планирования сервиса – Качества сервиса.

При разработке программного обеспечения можно использовать следующие механизмы:

Структурированная Система Разработки (Structured System Development)

Традиционная линейная (Traditional Linear)

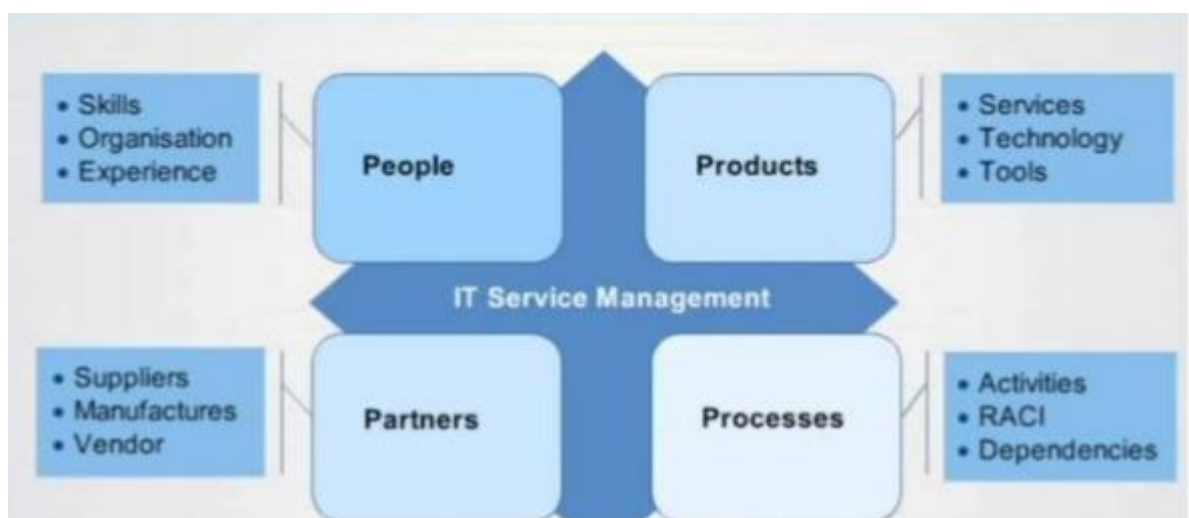
«Водопад» (Waterfall)

«V-Модель» (V-Model)

Быстрая Разработка (Rapid Application Development) – Быстрая разработка за счет повторного использования готовых и разработанных компонентов.

Коробочные Коммерческие Решения (Commercial Off-the-shell Solutions COTS)

Использование и адаптация коммерческих продуктов (COTS)



Выделяется пять ключевых аспектов Проектирования услуг

проектирование решений, в том числе всех требуемых и согласованных функциональных требований, ресурсов и возможностей;

проектирование поддерживающих управленческих систем и инструментов, в частности Портфеля услуг для управления и контроля услуг в рамках их жизненного цикла;

проектирование технологий, систем и инструментов управления, необходимых для предоставления услуг;

проектирование процессов, необходимых для построения дизайна, внедрения, эксплуатации и улучшения услуг;

проектирование методов и метрик для измерения качества, эффективности и производительности услуг, архитектур и процессов.

Прежде чем передать спроектированное решение на этап Внедрения, необходимо выполнить ряд дополнительных действий:

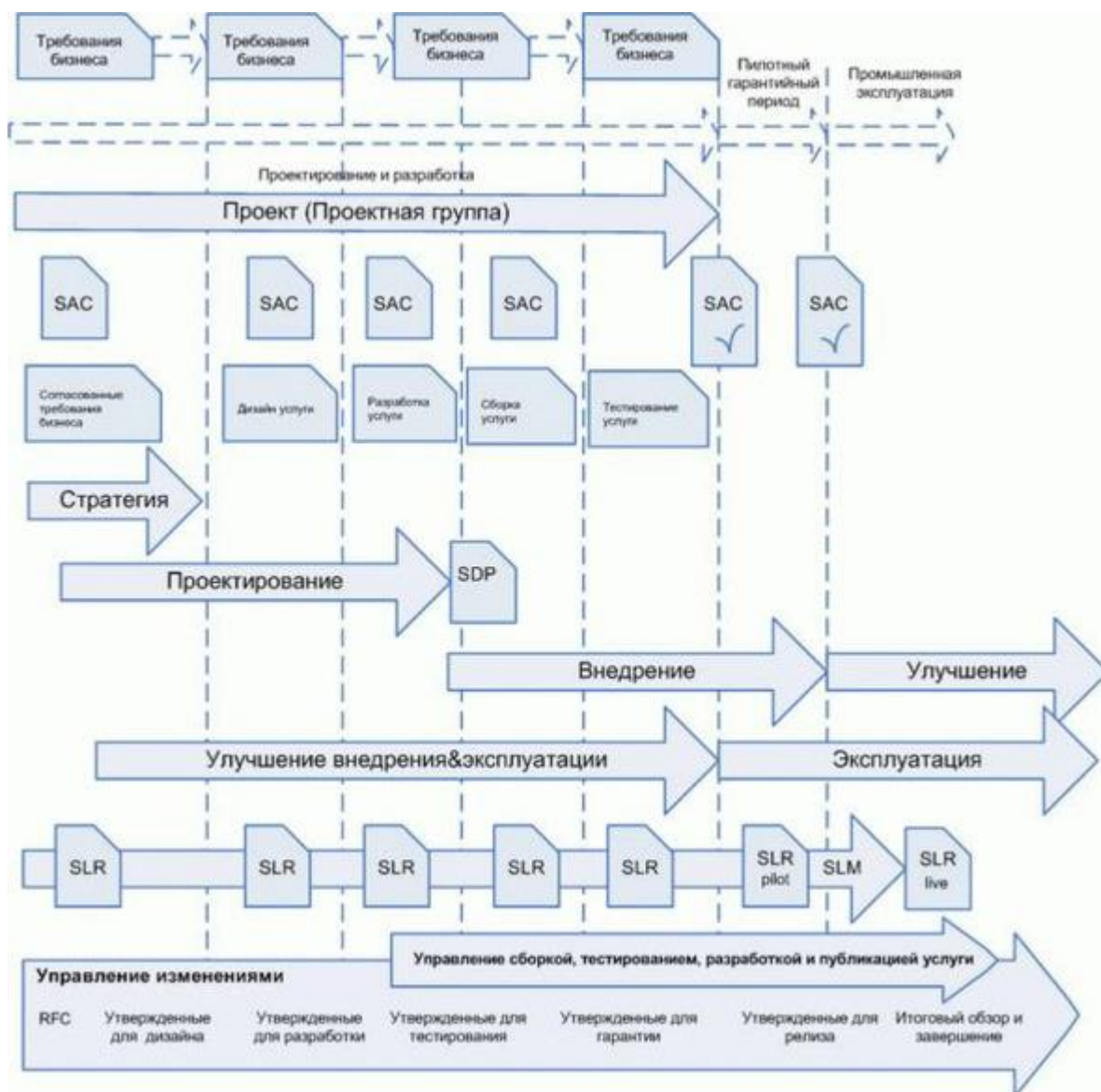
Оценка альтернативных решений. Эта деятельность необходима, если к предоставлению услуг привлечены внешние поставщики услуг и решений. Состоит из следующего:

формирование набора поставщиков и организация тендера;

обзор и оценка всех решений, предлагаемых поставщиками. Отбор наиболее подходящих для конкретной задачи поставщиков;

оценка и расчет стоимости альтернатив, с последующим выбором наилучших.

Снабжение выбранного решения



Хотя существует возможность, что для разработанного решения не потребуется участие третьих сторон (то есть поставщиков), тем не менее, на практике чаще всего они участвуют, а, следовательно, необходимо выполнить следующее:

- завершение всех необходимых проверок выбранного поставщика;
- заключение контрактов с поставщиком;
- снабжение выбранного решения.

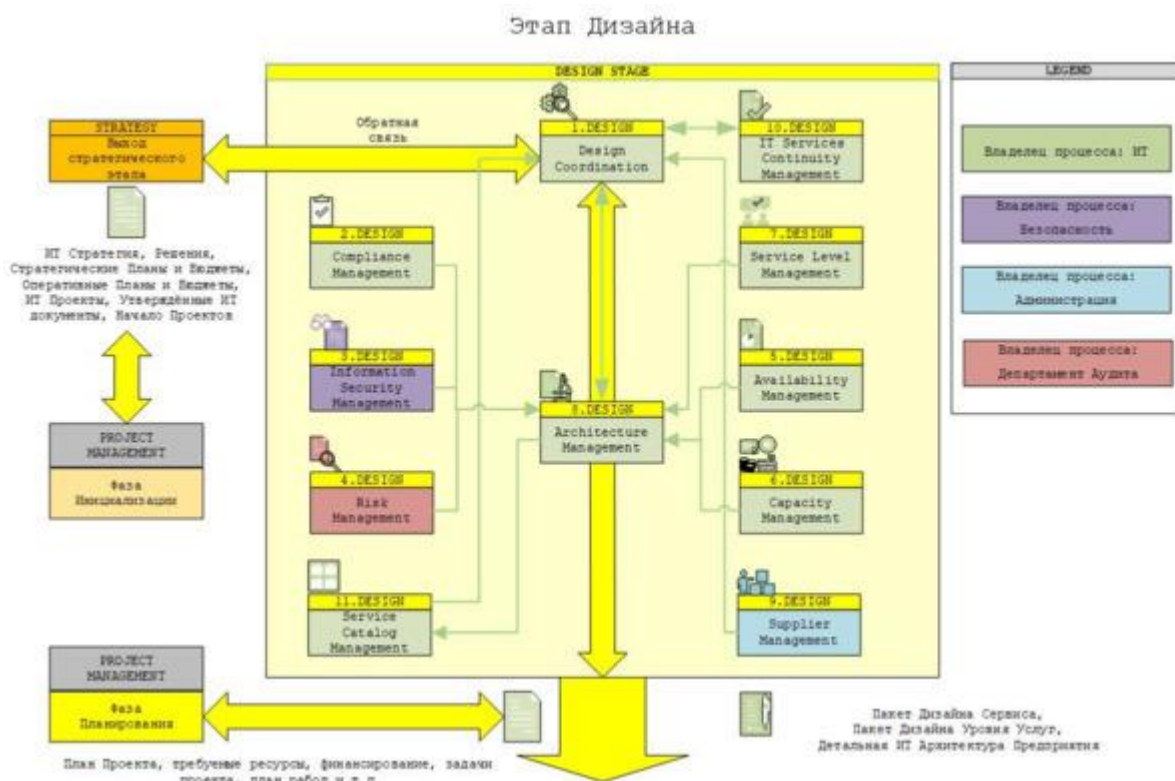
Разработка решения. Сюда относится деятельность по трансляции проекта услуги в план по ее разработке. Каждый план будет ответственен за разработку одного или более компонентов услуги и должен включать следующее:

- потребности бизнеса;
- стратегия, применяемая для разработки и/или приобретения решения;
- временные рамки;
- требуемые ресурсы, в том числе возможности и инфраструктуры ИТ, квалифицированный персонал и т. п.;
- разработка услуги и ее компонентов, в том числе механизмов управления, формирования отчетности, измерения и т. п.
- план тестирования услуги и ее компонентов.

Пакет Дизайна Сервиса (Service Design Package SDP)		
Категория	Под-категория	Описание
Требования (Requirements)	Бизнес требования (Business Requirements)	Первоначальные письменные бизнес требования согласованные и задокументированные
	Применимость сервиса (Service Applicability)	Определение как, когда и где данный сервис следует использоваться
	Контакты по сервису (Service Contacts)	Бизнес контакты с указанием владельца сервиса, исполнителей, проектной команды и т п
Дизайн сервиса (Service Design)	Функциональные требования (Functional Service Requirements)	Функциональные возможности предоставляемого сервиса, согласованные и задокументированные (Statement of Requirements SoR).
	Требования к Уровню Обслуживания сервиса (Service Level Requirements)	Требования к уровню сервиса (Service Level Requirements SLR) нового или обновленного соглашения (Service Level Agreement) включающие Гарантии Качества
	Требования к управлению и сопровождению (Service & Operational Management Requirements)	Требования по управлению сервисом и его компонентами включая поддержку, контроль, сопровождение, мониторинг, метрики и отчетность
	Дизайн и топология (Service Design & Topology)	Архитектура сервиса, план и порядок внедрения сервиса и его компонентов в «рабочую» среду.
Оценка организационных возможностей	Оценка организационных возможностей (Organizational Readiness Assessment)	Отчет и планирование, включающие в себя: оценка бизнес, финансовые, технические и организационные выгоды. Оценка требований, навыков, знаний необходимых для внедрения и сопровождения сервиса.
План жизненного цикла (Service Lifecycle Plan)	Программа жизненного цикла сервиса (Service Program)	Программа, покрывающая сопровождения сервиса на всех этапах жизненного цикла включая временные рамки.
	План внедрения сервиса (Service Transition Plan)	План внедрения с указанием стратегии, целей, задач, политик, и процедур. А также оценка рисков этапа внедрения.
	План сопровождения сервиса (Service Operational Acceptance Plan)	План сопровождения с указанием стратегии, целей, задач, политик, и процедур. А также оценка рисков этапа сопровождения сервиса.
	Критерии принятия сервиса (Service Acceptance Criteria)	Разработка и принятие критериев (Service Acceptance Criteria SAC) для оценки результатов на всех этапах жизни сервиса.

На выходе Сервис Дизайна формируется Пакет Сервис Дизайна (Service Design Package SDP), который включает в себя:

Процессы данного этапа формируют три основных документа: Пакет Дизайна Сервиса, Пакет Дизайна Уровня предоставления услуг
Детальную Архитектуру Предприятия.



На выходе, возможна корректировка стратегических планов и бюджетов. Пакеты решений передаются далее на этап Внедрения. В плане Управления Проектами принимается окончательное решение по началу проекта и выделение ресурсов, определения сроков ИТ проекта.

Координирование процесса Дизайна сервиса (Design Coordination DC)

Процесс Координирования Дизайна сервиса является главным на этапе Дизайна». Фактически процесс является аналогом процесса «Управления Изменениями» и отвечает на такие вопросы как:

- Формирование процесса дизайна сервиса.
- Координация деятельности различных процессов управления ИТ сервисами
- Интеграция фаз и процессов Управления Проектами

Деятельность по процессу:

- Утверждение процесса дизайна сервисов
- Координация деятельности по проектированию ИТ сервисов

Входы процесса:

- Выходы процессов Стратегического этапа
- Фаза инициализации Управление Проектами

Выходы процесса:

- Детальная ИТ Архитектура Предприятия
- Пакет Дизайна Сервиса
- Пакет Дизайна Предоставления Услуг
- Протокол решения ИТ комитета
- Необходимые данные для фазы планирования Управления Проектами

Участники процесса:

ИТ комитет
ИТ архитектор
Руководитель ИТ Проектов
Менеджер ИТ проектов
Экспертная группа, в составе которой эксперты и инженеры ИТ, представители бизнеса

Ключевые моменты процесса:
ИТ департамент является владельцем процесса

Назначение процесса (WHAT) и цели процесса (WHY):
Организация процесса дизайна сервиса
Организация дизайна сервиса

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):
Координация процессов дизайна ИТ сервисов
Координация требований Управления Проектами
Подготовка Пакетов Дизайна Сервиса и Предоставления Услуг
Утверждение Пакетов Дизайна Сервиса и Предоставления Услуг
Утверждение ИТ Архитектуры Предприятия

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

% требований спецификаций Сервис Дизайна предоставленных в срок и в соответствии с бюджетом

% Планов Сервис Дизайна предоставленных в срок и в соответствии с бюджетом

% Пакетов Сервис Дизайна законченных в срок

% соответствия бизнес требований и решений, сформированных в Пакетов Сервис Дизайна

% точности при оценке стоимости сервиса или проекта на этапе Сервис Дизайна

Управление Рисками (Risk Management RM)

Управление Рисками процесс этапа «Дизайна». Является ключевым процессом для организации. Данный процесс отвечает на такие вопросы как:

Формирование процесса управления рисками в рамках организации.

Формирование и утверждение реестра рисков

Расчет стоимости рисков

Анализ рисков и механизмов противодействия или снижения рисков

Формирование и утверждение реакции на риски

Порядок взаимодействия ИТ департамента с бизнесом по вопросам управления рисками

Порядок взаимодействия подразделений внутри ИТ департамента по вопросам управления рисками

Деятельность по процессу:

Формирование и утверждение процесса управления рисками

Формирование и утверждение реестра рисков

Формирование и утверждение реакции на риски

Выявление рисков

Определение владельцев рисков

Оценка рисков

Формирование реакции на риски

Внедрение реакции на риски

Gain assurances of effectiveness and efficiency

Embed and Review

Разработка и согласование процесса управления рисками

Исполнение требований комитета по управлению рисками

Определение рисков на всех этапах жизненного цикла сервиса

Решение Комитета по Управлению Рисками
Рекомендации по Информационной Безопасности

Входы процесса:

Процесс Управление Отношениями с Бизнесом
Процесс Управления Требованиями
ИТ архитектура
Contract Risks
Service Provider Risks
Design Risks
Transition Risks
Operational Risks
Market Risks

Выходы процесса:

Подписанный протокол решения ИТ комитета
Подписанный протокол решения Комитета по управлению Рисками
Risks responses

Участники процесса:

ИТ комитет
Комитет по управлению рисками
ИТ директор
ИТ архитектор
Руководители ИТ подразделений
Экспертная группа
Представители бизнеса
Представители комитета управления рисками
Представители департамента Безопасности

Ключевые моменты процесса:

Департамент Внутреннего ИТ Аудита (Комитет по Управлению Рисками) является владельцем процесса
Департамент ИТ является исполнителем (управляющим) по вопросам связанных с информационными технологиями.
Департамент Информационной Безопасности является консультантом в процессе

Назначение процесса (WHAT) и цели процесса (WHY):

Организация процесса управления рисками
Организация управления рисками

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

Организация процесса управления рисками
Согласование процесса управления рисками
Утверждение процесса управления рисками
Внесение изменений в процесс управления рисками
Проведение деятельности по обнаружению рисков
Проведение деятельности по анализу рисков
Формирование реестра рисков
Проведение деятельности по оценке рисков
Выработка мер противодействия рискам
Оценка мер противодействия рискам
Разрешение конфликта интересов по управления рисками

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

- Количество рисков
- Количество критических рисков
- Количество рисков по категориям

Управление ИТ Архитектурой (Architecture Management AM)

Управление ИТ архитектурой процесс этапа «дизайна». Является ключевым процессом для организации и ИТ департамента в частности. Данный процесс отвечает на такие вопросы как:

- Организация процесса Управления Архитектурой
- Разработка ИТ Архитектуры Предприятия
- Разработка Архитектуры ИТ сервисов

Архитектура предприятия должна включать в себя следующие основные архитектуры:

Архитектура услуг – транслирует приложения, инфраструктуры, организацию и поддержку деятельности в набор услуг. Архитектура услуг предоставляет независимый, интегрированный в бизнес подход для предоставления услуг бизнесу. Она предлагает модель для разделения между Архитектурой услуг, Архитектурой приложений, Архитектурой инфраструктуры и Архитектуры данных. В рамках Архитектуры услуг также рассматриваются вопросы обеспечения стойкости к сбоям, дальнейшей корректировки и обеспечения безопасности.

Архитектура приложений – предлагает детальный план по развитию и доставке индивидуальных приложений, отображает функциональные требования бизнеса к приложениям и показывает взаимозависимости между приложениями. Использование подхода, основанного на компонентах, максимизирует повторное использование и помогает приложениям быть гибкими в условиях изменяющихся политик снабжения.

Архитектура данных/информации – описывает логические и физические информационные активы организации, и ресурсы управления ими. Она показывает, как распределены информационные ресурсы и управление ими для достижения корпоративной цели.

Архитектура инфраструктуры – описывает структуру, функциональность и географическое распределение программного и аппаратного обеспечения, компонентов коммуникации, а также относящиеся к ним стандарты.

Архитектура окружения – описывает аспекты, уровни и типы контроля окружения, а также их управления.

Деятельность по процессу:

- Организация процесса управления Архитектурой

Входы процесса:

- Входы процессов стратегического этапа

Выходы процесса:

- ИТ Архитектура Предприятия
- Архитектура ИТ сервиса

Участники процесса:

- ИТ комитет
- ИТ архитектор
- Главы подразделений ИТ департамента
- Экспертная группа

Ключевые моменты процесса:

- ИТ департамент является владельцем процесса

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Управление Соответствиями Требованиям (Compliance)

Management COM)

Управление Соответствия Требованиям процесс этапа «дизайна». Процесс должен отвечает на такие вопросы как:

- Соответствие ИТ Архитектуры требованиям ИТ Стратегии
- Соответствие ИТ Архитектуры требованиям регуляторов
- Соответствие ИТ Архитектуры рекомендациям международных стандартов и практик

Деятельность по процессу:

- Назначение процесса (WHAT) и цели процесса (WHY):
- Организация процесса управления соответствия требованиям
- Сбор требований контролирующих органов
- Сбор рекомендаций международных стандартов и практик
- Анализ требований
- Разрешение конфликта интересов по соответствию требованиям

Входы процесса:

- Выходы процессов стратегического этапа
- Требования контролирующих органов
- Рекомендации международных стандартов и практик

Выходы процесса:

- Протокол решения ИТ комитета

Участники процесса:

- ИТ комитет
- ИТ архитектор
- Главы подразделений ИТ департамента
- Экспертная группа

Ключевые моменты процесса:

- ИТ департамент является владельцем процесса

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Управление Каталогом Сервисов (Service Catalog Management SCM)

Управление Каталогом Сервисов процесс этапа «Дизайна» и является частью процесса «Управления Портфелем Сервисов». В каталог сервисов находятся «рабочие» сервисы, т. е. сервисы которые находятся в эксплуатации и доступны для пользователей.

Цели процесса:

- Перечень сервисов, предоставляемых ИТ департаментом, находящиеся на этапе сопровождения.
- Управление информацией, содержащейся в каталоге услуг

Задачи процесса:

- Формирование каталога услуг, находящихся в эксплуатации
- Управление состояние каталога услуг,
- Организация взаимодействия с портфелем сервисов

Действия, которые должны быть предприняты в рамках Управления Каталогом услуг:

- Утверждение и документирование всех услуг вместе с компонентами, относящимися к ним;
- Взаимодействие с Управлением Портфелем услуг с целью согласования информации, содержащейся в Портфеле услуг и Каталоге услуг;
- Формирование и поддержка Каталога услуг с привязкой к Портфелю услуг;
- Взаимодействие с ИТ и бизнесом с целью установления зависимостей между бизнес-единицами с их бизнес-процессами и поддерживающими услугами.

•Взаимодействие со службами поддержки, поставщиками и Управлением конфигурациями с целью установления зависимостей между услугами и поддерживаемыми компонентами, содержащимися в Техническом Каталоге услуг.

Различают два вида сервисов:

Бизнес Сервис Каталог (Business Service Catalogue) – ИТ сервисы видимы и предоставляемые пользователям и клиентам

Технический Сервис Каталог (Technical Service Catalogue) – ИТ сервисы, обычно не видимые пользователям и клиентам

Основными входами процесса являются:

- стратегии и планы бизнеса и ИТ, текущие и будущие требования к Портфелю услуг;
- влияние, приоритеты и риски, связанные с каждой услугой или с изменением требований к ней. Эту информацию предоставляет процесс Анализа влияния на бизнес;
- требования бизнеса – детальное описание новых или измененных требований бизнеса к Портфелю услуг;
- Портфель услуг;
- Система управления конфигурациями (CMS);
- обратная связь с другими процессами в рамках жизненного цикла услуги.
- Процесс управления Портфелем Сервисов
- Процесс управления Взаимодействия с Бизнесом
- Процесс управления Портфелем Сервисов
- Процесс управления Взаимодействия с Бизнесом



Выходами процесса Управления Каталогом услуг являются:

- утвержденная руководством документация, описывающая услуги;
- обновления Портфеля услуг, в результате которых в нем будет содержаться актуальная информация о статусах и зависимостях услуг;
- Каталог услуг, который содержит детальное описание текущих статусов услуг, вместе с описанием интерфейсов и зависимостей.
- Подписанный протокол решения ИТ комитета

Участники процесса:

- ИТ комитет
- Менеджер по управлению портфелем сервисов

Ключевой показателя процесса:

- Процентное соотношение количества услуг, которые содержатся в Каталоге услуг, к количеству услуг, которые предоставляются заказчикам в определенный момент времени.
- Количество расхождений между информацией, содержащейся в Каталоге услуг, и «реальной ситуацией».

Ключевые моменты процесса:

- ИТ департамент является владельцем процессом.
- Каталог услуг для бизнеса связывает услуги и бизнес-процессы, то есть то, что волнует бизнес,
- Технический Каталог услуг связывает услуги с тем, что обеспечивает их работу, то есть то, что волнует ИТ.

Основными рисками для Управления Каталогом услуг является неточная информация, поступающая от бизнеса и ИТ, а также плохо организованный доступ к Каталогу услуг.

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

- Количество сервисов в каталоге
- Среднее время перехода сервиса из портфеля в каталог
- Среднее время нахождения сервиса в каталоге > 3 лет
- Отношение технических и бизнес сервисов > 70%
- Уровень полноты документирования сервиса > 70%

Управление Уровнем Предоставления Сервисов (Service Level Management SLM)

Управление Уровнем Сервисов процесс этапа «Дизайна». Является частью «Управления Портфелем Сервисов».

Управление уровнем услуг – процесс, ответственный за обсуждение Соглашений об уровне услуг, и гарантирующий их выполнение. Он ответственен за то, что процессы Управления услугами, соглашения операционного уровня и внешние договоры будут соответствовать согласованным целевым показателям уровня услуги. SLM является своего рода точкой взаимодействия поставщика услуг и заказчика.

Цели процесса:

- Организация процесса предоставления сервисов
- Согласование уровня предоставляемых сервисов.
- Обеспечение и улучшение взаимоотношений заказчиков и поставщиков;
- Обеспечение того, что целевые значения для услуг достижимы и их можно измерить;
- Мониторинг и улучшение удовлетворенности заказчиков уровнем предоставляемых услуг;
- Гарантия того, что заказчики имеют четкое и недвусмысленное ожидание уровня услуги;

Задачи процесса:

- развитие взаимоотношений с бизнесом;
- переговоры и согласование требований и целевых показателей, а также документирование и управление SLA для всех услуг, находящихся в промышленной эксплуатации.
- развитие и управление OLA, чтобы обеспечить соответствие и корреляцию с SLA.

- предупреждение отказов, уменьшение рисков, улучшение качества услуг;
- управление и отчетность по всем услугам, обзор всех слабостей и «брешей» SLA;
- координация Плана совершенствования услуг. План совершенствования услуг (Service Improvement plan) – формальный План для внедрения улучшений в процесс или услугу.

Основная деятельность в рамках процесса должна включать следующее:

- документирование, согласование, утверждение требований заказчиков в форме SLR и управление ими в рамках жизненного цикла услуги с помощью SLA;
- мониторинг и измерение производительности услуг в рамках SLA;
- измерение и мониторинг пользовательской удовлетворенности;
- формирование отчетности;
- сбор и анализ информации, полученной из отчетов; инициирование улучшений в рамках Плана совершенствования услуг;
- регистрация всех положительных и отрицательных отзывов;
- Формирование и утверждение процесса управления Уровнем Сервисов

Входами для процесса являются:

- информация от бизнеса – стратегии, планы, текущие и будущие требования;
- Анализ влияния на бизнес – информация о влиянии, приоритетах, рисках и количестве пользователей по каждой услуге;
- Портфель услуг и Каталог услуг;
- информация об изменениях – информация от процесса Управления изменениями;
- обратная связь с заказчиками, положительные и отрицательные отзывы.

Выходами процесса являются:

- отчеты об услугах, которые предоставляют информацию о работе услуги в контексте целевых показателей SLA. Эти отчеты должны содержать детальную информацию обо всех сторонах услуги и ее предоставления, включая текущую и прошлую производительность, слабости и «бреши», основные события, запланированные изменения, текущий и будущий объем работы, планы и деятельность по улучшению.
- План совершенствования услуг (SIP);
- шаблоны документов для составления SLA, SLR, OLA и других соглашений;

Участники процесса:

- ИТ комитет

При оценке процесса можно выделить следующие типы индикаторов:

субъективные индикаторы производительности.

- улучшение удовлетворенности заказчиков предоставляемыми услугами

объективные индикаторы производительности.

- количество или процент достигнутых целевых показателей;
- количество «брешей» в услугах;
- количество услуг с актуальными SLA;
- количество услуг с регулярно формируемыми отчетами и обзорами.

Управление уровнем сервисов базируется на важных документах:

- Соглашение об Уровне Услуг (Service Level Agreement SLA)
- Соглашение об Уровне Сопровождения (Operational Level Agreement OLA)
- Контрактах (Underpinning Contracts)

Соглашение об Уровне Услуг (Service Level Agreement SLA) – документированное и согласованное соглашение между ИТ сервис провайдером и клиентами. Различают:

- Соглашение на уровне сервиса (Service-based SLA)
- Соглашение на уровне пользователей (Customer-based SLA)
- Многоуровневое соглашение (Multi-level SLA)

Соглашение на уровне сервиса (Service-based SLA) – один сервис одно соглашение. Описывает один тип услуг для всех пользователей этой услуги. Например, услуга электронной почты для всех ее пользователей. Преимуществом данного подхода является его простота. Недостатком то, что разным типам пользователей может потребоваться разный уровень услуги или же они могут иметь различные преимущества с точки зрения инфраструктуры.

Соглашение на уровне пользователей (Customer-based SLA) – Одно соглашение на все сервисы для одного клиента.

Многоуровневое соглашение (Multi-level SLA) – Соглашение на уровне организации и т. п. и может включать три уровня:

- уровень корпорации – покрывает базовые особенности, подходящие для каждого сотрудника организации.
- уровень пользователей – покрывает все особенности, относящиеся к конкретной группе пользователей или бизнес-единице в части используемых ими услуг;
- уровень услуг – покрывает все особенности, относящиеся к конкретной услуге в отношении конкретной группы пользователей.

Соглашение об Уровне Сопровождения (Operational Level Agreement OLA) – документированное и согласованное соглашение между ИТ сервис провайдером и третьей стороной той же организации, что оказывает содействие в предоставлении сервисов. Как пример может быть соглашение с ИТ департамента с административным департаментом, обслуживающим инженерные службы и системы обеспечения.

В качестве требований предъявляемым к SLA и шагам можно отнести:

- формулировка SLA должна быть ясной и полной.
- Утверждение формы SLA,
- Нахождения баланса между тем, что хочется, и тем, что объективно возможно обеспечить.
- Разработать механизмы для мониторинга.

Измерение пользовательской удовлетворенности отлично от измерения производительности, которую можно и нужно максимально автоматизировать. Пользовательская удовлетворенность является субъективным фактором.

Удовлетворенность пользователей = восприятие – ожидания. Если это значение нулевое или больше нуля, то заказчик удовлетворен.

Чтобы измерить восприятие заказчика можно использовать следующие методы и средства:

- периодические опросы и анкетирование;
- обратная связь
- телефонный опросы;
- анализ достоинств и недостатков.

Обзор результатов внедрения является частью процесса Управления изменениями. Обзор результатов внедрения (Post Implementation Review или PIR) – обзор, выполняемый после внедрения изменения проекта. Он определяет успешность изменения проекта и выявляет возможности для улучшения.

Для поставщика услуг важно показать заказчикам то, что он внимательно относится к их мнению и вносит соответствующие коррективы и улучшения в предоставляемые услуги.

Типовая модель Service Level Agreement должно включать следующие разделы:

- Определение предоставляемого сервиса, стороны, вовлеченные в соглашение, и сроки действия соглашения.
- Дни и часы, когда сервис будет предлагаться, включая тестирование, поддержку и модернизации.
- Число и размещение пользователей и/или оборудования, использующих данный сервис.
- Описание процедуры отчетов о проблемах, включая условия эскалации на следующий уровень. Должно быть включено время подготовки отчета.
- Описание процедуры запросов на изменение. Может включаться ожидаемое время выполнения этой процедуры.
- Спецификации целевых уровней качества сервиса, включая:

°Средняя доступность, выраженная как среднее число сбоев на период предоставления сервиса

°Минимальная доступность для каждого пользователя

°Среднее время отклика сервиса

°Максимальное время отклика для каждого пользователя

°Средняя пропускная способность

°Описания расчета приведенных выше метрик и частоты отчетов

•Описание платежей, связанных с сервисом. Возможно, как установление единой цены за весь сервис, так и с разбивкой по уровням сервиса.

•Ответственности клиентов при использовании сервиса (подготовка, поддержка соответствующих конфигураций оборудования, программного обеспечения или изменения только в соответствии с процедурой изменения).

•Процедура разрешения конфликтов.

Множество факторов может послужить триггерами для внесения изменений в сервисное соглашение:

- изменения в Портфеле услуг,
- Новые требования бизнеса,
- Новые требования регулятора,
- Новые или измененные услуги;
- нарушения в услуге;
- положительные или отрицательные отзывы;
- изменения в стратегии или политиках.

Управление Доступностью (Availability Management AVM)

Управление Доступностью является процессом этапа «дизайна». Является ключевым процессом для организации и ИТ департамента в частности.

Доступность (Availability) – способность конфигурационной единицы или услуги выполнять согласованную функцию, когда это требуется. Доступность определяется через надежность, сопровождаемость, обслуживаемость, производительность и безопасность.

Управление доступностью (Availability Management) – процесс, отвечающий за определение, анализ, планирование, измерение и улучшение всех аспектов доступности услуги. Управление доступностью отвечает за то, чтобы вся инфраструктура, процессы, средства, роли и т. д. соответствовали согласованным Целевым показателям уровня услуги в части Доступности.

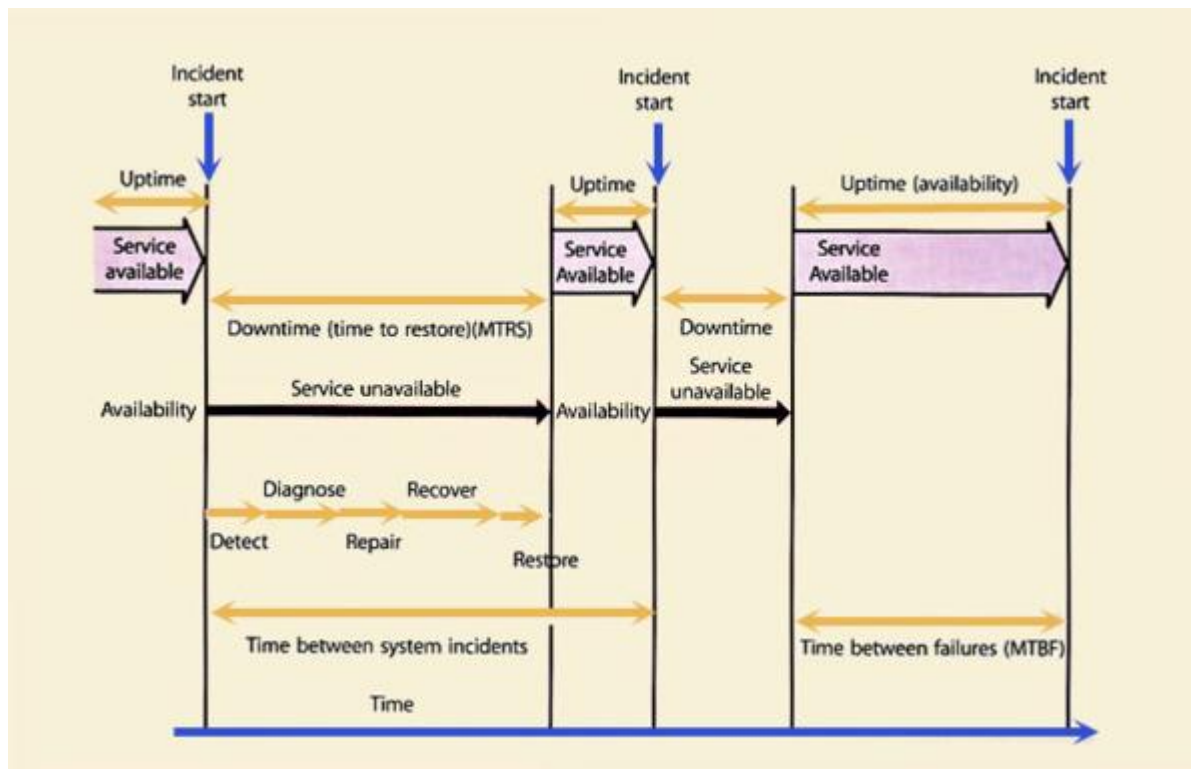
План управления доступностью (Availability Plan) – план, обеспечивающий эффективное по затратам выполнение текущих и будущих требований доступности к услуге;

Цели процесса:

- Формирование процесса Управления Доступностью
- Гарантирование согласованного уровня доступности сервиса
- гарантия того, что уровень доступности услуг эффективен по затратам и соответствует текущим или будущим потребностям бизнеса
- Непрерывная оптимизация и улучшение доступности

Процесс Управления доступностью должен включать в себя следующие деятельности:

- Формирование плана управления доступностью
- Предоставление рекомендации и руководства для других областей бизнеса и ИТ по всем вопросам, связанным с доступностью;
- содействие в идентификации и разрешении всех проблем и вопросов, связанных с недоступностью услуг и их компонентов.
- Сбор и анализ состояния сервисов
- Определение ключевых показателей доступности сервиса



Входами процесса Управления доступностью являются:

- информация от бизнеса – стратегия, планы и бюджет организации, ее текущие и будущие требования, в том числе требования к доступности новых или измененных услуг;
- информация от Анализа влияния на бизнес,
- информация об услугах от Портфеля услуг и Каталога услуг;
- финансовая информация – стоимость предоставления услуг и затраты на ресурсы;
- информация о релизах и изменениях
- информация от Управления конфигурациями
- целевые показатели услуг

Выходами процесса Управления доступностью являются:

- План управления доступностью;
- критерии для проектирования доступности, предлагаемые целевые показатели;
- отчеты о доступности, надежности и сопровождаемости услуг в контексте достижения ими целевых показателей;

Для оценки эффективности процесса Управления доступностью можно использовать множество ключевых показателей производительности:

Управление доступностью и надежностью услуг:

- процентное уменьшение недоступности услуг и их компонентов
- процентное увеличение надежности услуг и их компонентов
- эффективный пересмотр SLA, OLA и других основополагающих контрактов, и договоров;
- процентное улучшение конечной доступности услуг;
- процентное уменьшение количества сбоев
- улучшение MTBF;
- улучшение MTBSI;
- улучшение MTRS.

Удовлетворение потребностей бизнеса в доступности услуг:

- процентное уменьшение недоступности услуг;
- процентное уменьшение стоимости простоя
- процентное уменьшение сбоев
- процентное увеличение удовлетворенности бизнеса.

Оптимальные затраты на обеспечение доступности услуг:

- процентное уменьшение стоимости недоступности;
- своевременный анализ рисков и обзора системы;
- процентное уменьшение сбоев услуг третьих сторон;
- своевременное формирование управленческих отчетов.

Ключевые моменты процесса:

- ИТ департамент является владельцем процесса

Управление доступностью включает в себя про активные и реактивные действия.

Реактивные действия заключаются в мониторинге, измерении, анализе, формировании отчетов и обзоров обо всех аспектах, связанных с доступностью. Они гарантируют то, что целевые показатели доступности достигнуты и измерены.

Про активные действия заключаются в формировании рекомендаций, планов, документов для проектирования и критериев для новых или измененных услуг. Сюда также входят действия по постоянному улучшению услуг и уменьшению рисков там, где это экономически оправдано.

Управление доступностью состоит из двух взаимосвязанных уровней:

•доступность услуг – включает в себя все вопросы, связанные с доступностью и недоступностью услуг, а также влияние доступности (или недоступности) отдельных компонентов на доступность услуг в целом.

•доступность компонентов – включает в себя все вопросы, связанные с доступностью и недоступностью компонентов.

Управление доступностью основано на мониторинге, анализе, измерении и формировании отчетов о следующих компонентах:

Доступность (AVAILABILITY) – определяет возможность сервиса выполнять согласованные функции:

$$AVAILABILITY (\%) = ((AGREED SERVICE TIME - Downtime) / AGREED SERVICE TIME) \times 100$$

Надежность (RELIABILITY) – мера того, как долго услуга, компонент или конфигурационная единица может выполнять согласованную функцию без прерывания. Надежность услуги можно повысить двумя способами. Первый заключается в повышении устойчивости услуги к отказу отдельных компонентов, второй – в увеличении надежности отдельных компонентов.:

$$RELIABILITY (MTBSI \text{ часы}) = AVAILABILITY \text{ Time (часов)} / \text{Number of breaks}$$

Среднее Время Между Инцидентами Сервиса (Mean Time Between Service Incidents MTBSI)

$$RELIABILITY (MTBF \text{ часы}) = (AVAILABILITY \text{ Time (часов)} - TOTAL DOWNTIME) / \text{Number of breaks}$$

Среднее Время Между Отказами (Mean Time Between Failures MTBF)

Сопровождаемость / Ремонтопригодность (MAINTAINABILITY) – параметр, который определяет, как быстро и эффективно сервис или его компоненты могут быть восстановлены до нормального уровня после сбоя:

$$\text{MAINTAINABILITY (MTRS часы)} = \text{TOTAL DOWNTIME (часов)} / \text{Number of breaks}$$

Среднее Время на Восстановление Сервиса (Mean Time to Restore Service MTRS)

Обслуживаемость / Удобство эксплуатации (SERVICEABILITY) – параметр, который определяет, возможность третьей стороны (supplier) выполнять свои обязательства в рамках согласованных сроков, установленных в контракте. Тот договор будет включать в себя согласованные уровни надежности, Сопровождаемость или доступности для конфигурационной единицы.

В контексте процессов Проектирования вводится также термин:

Критичная бизнес-функция (Vital Business Function VBF) – функция в бизнес-процессе, критичная для успеха Бизнеса. Чем выше критичность функции для бизнеса, тем большую надежность и доступность в отношении нее необходимо обеспечить. Некоторые VBF требуют особого подхода при проектировании обслуживающих их услуг:

- *Устойчивость (RESILIENCE)* – параметр, который определяет, возможность сервиса выполнять свои функции при отказе или прерывании одного, или нескольких компонентов сервиса.

- *Высокая Доступность (High Availability HA)* – уменьшение или скрывание эффекта от отказа компонентов сервиса.

- *Отказоустойчивость (Fault Tolerance)* – возможность ИТ сервиса выполнять свои функции даже после отказа компонентов сервиса.

- *Непрерывная работа (Continuously Operation)* – действия по снижению влияния запланированного простоя и обслуживания сервиса.

- *Непрерывная Доступность (Continuously Availability)* – действия по достижению 100% доступности сервиса.

Основным риском для процесса Управления доступностью, также, как и для предыдущих процессов, является недостаточность или неточность информации, поступающей от бизнеса и ИТ.

Управление Мощностями (Capacity Management CAM)

Управление Мощностями является процессом этапа «дизайна». Является ключевым процессом для организации и ИТ департамента в частности.

Процесс Управление мощностями отвечает за своевременное и эффективное по затратам соответствие мощности услуг и инфраструктуры требованиям согласованных целевых показателей уровня услуги.

Мощность (Capacity) – максимальная пропускная способность, которую может обеспечить конфигурационная единица или услуга в рамках согласованных целевых показателей уровня услуги. Для некоторых типов конфигурационных единиц, мощность может быть выражена размером или объемом, например, жесткого диска.

Цели процесса:

- Формирование процесса Управления Мощностями

- Поддержание ИТ инфраструктуры на требуемом уровне

- Балансирование стоимости и ресурсов

- Балансирование снабжения и требований

- формировать План обеспечения мощностей и управлять им. *План обеспечения мощностей (Capacity Plan)* – план обеспечения мощностей используется для управления ресурсами, необходимыми для предоставления услуг. Этот план содержит сценарии для прогнозирования

спроса со стороны Бизнеса, и оценку затрат, необходимых для обеспечения согласованных Целевых показателей уровня услуги;

- предоставлять рекомендации и руководства для всех других областей бизнеса и ИТ по всем вопросам, связанным с производительностью и мощностью;
- содействовать в диагностировании и разрешении проблем, связанных с производительностью и мощностью;
- оценивать влияние изменений на План обеспечения мощностей, услуги и ресурсы;
- гарантировать, что про активные средства улучшения производительности внедрены там, где это экономически оправдано.

Задачи процесса:

- баланс затрат и требуемых ресурсов – обеспечивать то, чтобы производительность процессов была оправдана с точки зрения затрат на них, и обеспечивать наиболее эффективное использование ресурсов.
- баланс спроса и предложения – следить, чтобы предоставляемые ИТ предложения удовлетворяли спросу со стороны заказчиков в настоящем и будущем.

Управление мощностями включает в себя следующие деятельности:

- мониторинг моделей бизнеса-деятельностей и планов на уровне услуг в терминах производительности использования пропускной способности ИТ-услуг и поддерживающих инфраструктур, окружения, данных, приложений. Процесс должен формировать случайные и регулярные отчеты о производительности и мощности услуг и их компонентов;
- проведение деятельности по регулировке и настройке с целью максимально эффективного использования ресурсов;
- понимание утвержденных и будущих требований заказчиков в ИТ-ресурсах, формирование прогнозов относительно требований в будущем;
- формирование Плана обеспечения мощностей;
- содействие в диагностировании проблем и инцидентов
- про активное улучшение услуг и их компонентов там, где это экономически оправдано или требуется бизнесом.
- Формирование процесса управления Мощностями

Выделяют реактивные и про активные мероприятия в рамках процесса Управления мощностями.

К *про активные мероприятия* относятся:

- «предугадывание» появления вопросов, связанных с нехваткой ресурсов;
- выделение тенденций использования ресурсов в настоящее время и оценка будущих требований к ресурсам.
- моделирование и анализ тенденций изменений в ИТ-услугах, в том числе определение изменений в ресурсах, которые должны быть предприняты в будущем;
- обеспечение того, что обновления будут профинансированы, запланированы и проведены до того, как будет нарушен SLA или появятся какие-то проблемы с производительностью;
- активный поиск возможностей для улучшения производительности услуг там, где это экономически оправдано;
- настройка и оптимизация производительности услуг и их компонентов.

К *реактивным мероприятиям* относятся:

- мониторинг, измерение и ведение отчетности по текущей производительности услуг и их компонентов;
- реагирование на все события, связанные с пороговыми величинами производительности, и дальнейшая инициализация коррективных мер;
- реагирование на все проблемы, связанные с производительностью и помощь в их разрешении.

В рамках Управления мощностями выделяют три под-процесса:

- Управление мощностями бизнеса – транслирует потребности и планы бизнеса в требования к услугам и инфраструктуре;

- Управление мощностями услуг – управляет, контролирует и предсказывает производительность и мощность услуг, находящихся в эксплуатации;

- Управление мощностями компонентов – управляет, контролирует и предсказывает производительность и мощность отдельных компонентов.

Чем эффективнее проводятся про активные мероприятия, тем меньше потребуется реактивных действий со стороны Управления мощностями. Действия в рамках каждого из рассмотренных под процессами отличаются. Главным отличием является информация, которая отслеживается и собирается. Например, уровень утилизации отдельных компонентов – процессоров, дисков, сетевого оборудования – вопросы Управления мощностью компонентов. Транзакция между показателями пропускной способности и временем ответа – вопросы Управления мощностью услуг. К вопросам Управления мощностями бизнеса относятся транзакция между показателями онлайн-услуг и бизнес-объемов – например, в терминах увеличения продаж или обслуженных ордеров.

Входами процесса Управления мощностями являются:

- информация от бизнеса – стратегии и планы организации, ее текущие и будущие требования;
- информация от ИТ – стратегии, планы и бюджет ИТ. Эта информация покрывает все вопросы, связанные с технологиями, инфраструктурой, окружением, данными и приложениями, и их связи со стратегиями и планами бизнеса;

- информация о производительности и мощности компонентов;

- проблемы, связанные с производительностью услуг – инциденты и проблемы, связанные с плохой производительностью;

- информация о услугах – информация от SLM, в том числе от Каталога услуг и Портфеля услуг, целевые показатели услуг в SLA и SLR, и т. п.

- финансовая информация – информация от процесса Управления финансами, в том числе стоимость предоставления услуг, ресурсов, компонентов и обновлений; выгода для бизнеса, финансовые планы и бюджет; затраты, связанные с отказом услуг или их компонентов.

- информация об изменениях: от процесса Управления изменениями, в том числе расписание изменений, оценка влияния изменений на мощность.

Выходами Управления мощностями являются:

- План обеспечения мощностей;

- информация и отчеты о производительности услуг

- анализ рабочей нагрузки и отчеты по ней.

- прогнозы, которые используются всеми областями для анализа и прогнозирования, в особенности руководством при принятии решений.

Участники процесса обсуждения и принятия решений:

- ИТ архитектор

- Главы подразделений ИТ департамента

- Экспертная группа

Показатели, которые оценивают эффективность Управления мощностями, должны включать:

- Точные бизнес-прогнозы;

- Своевременное прогнозирование рабочей нагрузки;

- Точность прогнозов относительно бизнеса;

- Объединение бизнес-планов с Планом обеспечения мощностей;

- Уменьшение расхождений между бизнес-планами и Планом обеспечения мощностей.

- улучшение мониторинга производительности услуг

- уменьшение случаев «покупки чего-то в последний момент» для решения срочных проблем с производительностью;

- уменьшение функционирования услуг и компонентов на грани своих возможностей по производительности и мощности;

- уменьшение случаев нарушений в бизнес-процессах, вызванных нехваткой мощности со стороны ИТ;
- уменьшение инцидентов, связанных производительностью.

Ключевые моменты процесса:

- ИТ департамент является владельцем процесса

Количество информации, формируемой в рамках Управления мощностями, огромно и, как следствие, трудно поддается анализу. Поэтому необходимо сосредотачивать усилия на наиболее важных ресурсах и вопросах их использования.

Количество информации, формируемой в рамках Управления мощностями, огромно и, как следствие, трудно поддается анализу. Поэтому необходимо сосредотачивать усилия на наиболее важных ресурсах и вопросах их использования.

Управление Непрерывностью ИТ Сервисов (IT Service Continuity Management SCO)

Управление Непрерывностью ИТ сервисов является процессом этапа «дизайна». Является ключевым процессом для организации и ИТ департамента в частности. Управление непрерывностью услуг – процесс, ответственный за управление рисками, которые влияют на услуги. ITSCM обеспечивает возможность поставщику услуг постоянно предоставлять минимально согласованный Уровень услуг, через снижение рисков до приемлемого уровня и Планирование восстановления услуг.

Управление Непрерывностью ИТ Сервисов (IT Service Continuity Management SCO)

Управление непрерывностью услуг – процесс, ответственный за управление рисками, которые влияют на услуги. ITSCM обеспечивает возможность поставщику услуг постоянно предоставлять минимально согласованный Уровень услуг, через снижение рисков до приемлемого уровня и Планирование восстановления услуг.

Основная цель Управления непрерывностью услуг – поддерживать процесс Управления непрерывностью бизнеса.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса Управления непрерывностью ИТ сервисов
- Поддержание ИТ инфраструктуры на требуемом уровне
- Соответствие ИТ инфраструктуры требованиям бизнеса
- предоставление рекомендаций и руководств другим областям ИТ в вопросах, связанных с непрерывностью и восстановлением услуг;
- обеспечение механизмов непрерывности и восстановления, которые позволят достигнуть целевых показателей, установленных бизнесом;

Деятельность в рамках процесса Управления непрерывностью:

- Согласование границ ITSCM и применяемых политик;
- Анализ влияния на бизнес для количественной оценки влияния потери услуги на бизнес; *Анализ рисков* – идентификация и оценка рисков с целью определения потенциальных угроз непрерывности и оценки вероятности их осуществления. Сюда также входит применение механизмов управления угрозами там, где это экономически эффективно;
- формирование стратегии ITSCM, интегрированной в стратегию BCM.
- формирование Планов обеспечения непрерывности, интегрированных в планы BCM.
- Тестирование планов обеспечения непрерывности;
- Формирование процесса управления Непрерывностью ИТ сервисов

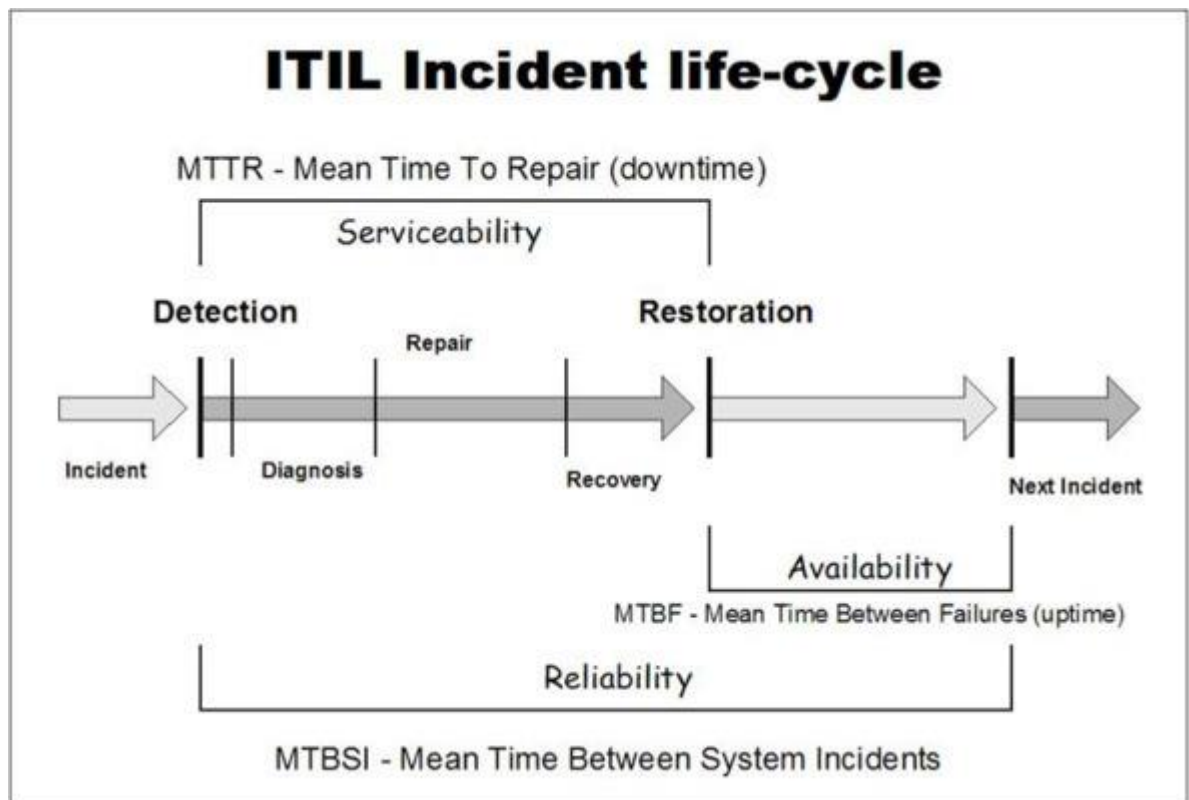


Диаграмма непрерывности сервиса – жизненный цикл инцидента

Фазы Процесса Управления Непрерывностью ИТ Сервисов включают в себя:

Инициализация (Initialization) – Начальная фаза

Определение политик

Определение условий и области применения

Аудит, меры предосторожности и т.п.

Распределение ресурсов

Определение организации проекта и структуру контроля

Согласование плана проекта и качества

Определение механизма коммуникации

Фаза определения требований (Requirements)

Формирование бизнес требований

Риск анализ (Risk Analysis)

Анализ Воздействия на Бизнес

Определение стратегии непрерывности ИТ сервиса

Определение стратегии оценки и реагирования на риски

Определение стратегии внешней площадки

Определение стратегии восстановления

Обходные действия

Взаимная договоренность

Постепенное восстановление

Промежуточное восстановление

Быстрое восстановление

Немедленное восстановление

Внедрение (Implementation) – фаза внедрения

Текущие операции (Ongoing Operation) – фаза сопровождения сервиса

Обучение

Обзор

Тестирование

Основные мероприятия по обеспечению Управления Непрерывностью Сервиса:

- проводится регулярный аудит планов ITSCM с целью проверки того, что требования бизнеса к восстановлению могут быть удовлетворены;
- все целевые показатели восстановления услуг документированы, согласованы в SLA и могут быть достигнуты с помощью планов ITSCM;
- проводится регулярное и всеобъемлющее тестирование планов ITSCM;
- обеспечивается уменьшение рисков и негативного влияния сбоев услуг.

Входами Процесса Управления Непрерывностью ИТ Сервисов являются:

- информация от бизнеса – стратегия, планы и бюджет организации, текущие и будущие требования;
- информация от ИТ – стратегия, планы и бюджет ИТ;
- стратегия и планы обеспечения непрерывности бизнеса;
- информация об услугах
- финансовая информация
- информация об изменениях
- информация о взаимоотношениях бизнеса с услугами
- Управление Требованиями
- Управление Доступностью
- Ключевые показатели доступности сервиса

Выходами Процесса Управления Непрерывностью ИТ Сервисов являются:

- политика и стратегия ITSCM;
- набор планов, в том числе планы Антикризисного управления, Срочных ответных действий, Восстановления после катастрофы, а также совокупность вспомогательных планов и контрактов с поставщиками услуг по восстановлению.
- Анализ влияния на бизнес и соответствующие отчеты;
- Анализ рисков и управленческие обзоры и отчеты;
- расписание тестирования ITSCM;
- сценарии для проведения тестирования;

Участники процесса обсуждения и принятия решений:

- ИТ архитектор
- Главы подразделений ИТ департамента
- Экспертная группа

Ключевым показателем производительности ITSCM является то, что предоставляемые услуги могут быть восстановлены с целью поддержки бизнеса в достижении поставленных целей.

В качестве показателя эффективности может также выступать готовность организации к действиям в соответствии с планами ITSCM.

Ключевые моменты процесса:

- ИТ департамент является владельцем процесса

Основными рисками для ITSCM являются недостаточность и некорректность информации, поступающей от бизнеса, ИТ и других процессов, а также нехватка ресурсов для обеспечения непрерывности.

Управление Информационной Безопасностью (Information Security Management ISM)

Управление информационной безопасностью – процесс, который обеспечивает конфиденциальность, целостность и доступность активов, информации, данных и услуг организации. Управление информационной безопасностью обычно является частью Организационного подхода к Управлению безопасностью, который имеет более широкую область охвата, чем поставщик услуг, и включает обработку бумажных документов, доступ в здания, телефонные звонки и т. п., для всей организации.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса Управления Информационной Безопасностью
- Поддержание ИТ инфраструктуры на требуемом уровне
- Соответствие ИТ инфраструктуры требованиям Информационной Безопасности
- Определение политик и процедур по мониторингу активности
- Определение политик и процедур по расследованию инцидентов
- Формирование требований и рекомендации по вопросам Информационной Безопасности

Основной целью является обеспечение эффективного управления информационной безопасностью всех услуг и деятельности в рамках Управления услуг. Информационная безопасность предназначена для защиты от нарушения конфиденциальности, доступности и целостности информации, информационных систем и коммуникаций.

Цель обеспечения информационной безопасности достигнута, если:

- Информация доступна тогда, когда это требуется, а информационные системы устойчивы к атакам, могут избегать их или быстро восстанавливаться.
- Информация доступна только тем, кто имеет соответствующие права.
- Информация корректна, полна и защищена от неавторизованных изменений.
- Обмен информацией с партнерами и другими организациями надежно защищен.

Ключевые деятельности в рамках процесса:

- формирование, пересмотр и корректирование Политики информационной безопасности и набора поддерживающих ее вспомогательных политик;
- реализация и соблюдение политик информационной безопасности, а также обеспечение взаимодействия между ними;
- оценка и классификация всех информационных активов и документов;
- использование, пересмотр и корректирование набора контролей безопасности, мер по оценке рисков и ответных действий;
- мониторинг и управление «брешами» безопасности и инцидентами;
- анализ, ведение отчетности и уменьшение влияния «брешей» в безопасности и инцидентов;
- составление расписания и проведение аудитов, тестирования и обзоров.
- Разработка и согласование процесса управления Информационной Безопасностью

Процесс должен включать в себя:

- формирование, управление, распространение и соблюдение Политики информационной безопасности и других вспомогательных политик, которые имеют отношение к информационной безопасности. *Политика информационной безопасности (Security Policy)* – политика, определяющая подход организации к управлению информационной безопасностью.

- понимание согласованных текущих и будущих требований бизнеса к безопасности;
- использование контролей безопасности для выполнения Политики информационной безопасности и управления рисками, связанными с доступом к информации, системам и услугам. В данном контексте контроль безопасности означает набор контрмер и мер предосторожности, применяемых для аннулирования, уменьшения рисков и противостояния им.
- про активное улучшение контролей безопасности и уменьшение рисков нарушения информационной безопасности;
- интеграция аспектов информационной безопасности во все процессы Управления услуг.

Политика информационной безопасности должна включать в себя следующее:

- реализация аспектов Политики информационной безопасности;
- возможные злоупотребления аспектами Политики информационной безопасности;
- политика контроля доступа;
- политика использования паролей;
- политика электронной почты;
- политика интернета;
- политика антивирусной защиты;
- политика классификации информации;
- политика классификации документов;
- политика удаленного доступа;

Перечисленные политики должны быть доступны пользователям и заказчикам, которые в свою очередь обязаны письменно подтвердить свое согласие с ними.

Политики утверждаются руководством бизнеса и ИТ и пересматриваются в зависимости от обстоятельств.

Пять элементов процесса управления Информационной Безопасностью:

- Контроль.
- Планирование.
- Реализация
- Оценка.
- Поддержка.

Контроль. Цели контроля:

- формирование системы управления информационной безопасностью в рамках организации;
- формирование организационной структуры для подготовки, утверждения и реализации Политики информационной безопасности;
- распределение ответственностей;
- формирование документации по контролю.

Планирование. Цель планирования – разработать и рекомендовать подходящие метрики и способы измерения информационной безопасности. В первую очередь планирование должно учитывать требования и особенности конкретной организации. Источниками информации для формирования требований к информационной безопасности являются бизнес, риски, планы, стратегия, соглашения (в первую очередь OLA и SLA). При этом важно учитывать моральную, законодательную и этическую ответственности в контексте информационной безопасности.

Реализация. Цель реализации – обеспечение подходящих процедур, инструментов и контролей безопасности для поддержки Политики информационной безопасности. В рамках реализации проводятся следующие мероприятия:

- идентификация активов;

- классификация информации

Оценка. Цель оценки:

- проверка соответствия политики информационной безопасности требованиям к информационной безопасности из SLA и OLA;
- проведение регулярных проверок технической составляющей информационной безопасности для IT систем;
- предоставление информации для регуляторов и внешних аудиторов при необходимости;

Поддержка. Цели поддержки:

- улучшение соглашений в отношении информационной безопасности, например, SLA и OLA
- совершенствование средств и контролей информационной безопасности.



Входами процесса являются:

- информация от бизнеса – стратегии, планы, бюджет бизнеса, а также его текущие и будущие требования;
- информация от IT – стратегия, планы и бюджет IT;
- информация об услугах
- отчеты процессов и анализа рисков
- детальная информация обо всех инцидентах информационной безопасности и «брешах» в ней;
- информация об изменениях
- информация о взаимоотношениях бизнеса с услугами
- ИТ архитектура

Выходами процесса являются:

- всеобъемлющая Политика информационной безопасности и другие вспомогательные политики, которые имеют отношение к информационной безопасности;

- Система управления информационной безопасностью (ISMS), которая содержит всю информацию, необходимую для обеспечения ISM;
- набор контролей безопасности, описание их эксплуатации и управления, а также всех связанных с ними рисков;
- аудиты информационной безопасности и отчеты;
- расписание тестирования планов информационной безопасности;
- классификация информационных активов;
- Политики, процедуры и стандарты по вопросам Информационной Безопасности

Участники процесса обсуждения и принятия решений:

ИТ комитет,
ИТ директор
ИТ архитектор
Руководители ИТ подразделений
Экспертная группа
Представители бизнеса
Представители комитета управления рисками
Представители департамента Безопасности
Представители департамента внутреннего аудита

В качестве ключевых показателей производительности процесса Управления информационной безопасностью можно использовать множество метрик:

- защищенность бизнеса от нарушений информационной безопасности
- процентное уменьшение сообщений о «брешах»
- процентное увеличение пунктов, касающихся информационной безопасности, в SLA.
- формирование четкой и согласованной политики информационной безопасности, учитывающей потребности бизнеса, то есть уменьшение количества несовпадений между процессами ISM и процессами, и политиками информационной безопасности бизнеса.
- увеличение согласованности и пригодности процедур обеспечения безопасности;
- увеличение поддержки со стороны руководства

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Количество инцидентов ИБ

Количество обнаруженных атак

Количество обнаруженных проникновений

Количество нарушений политики паролей

Количество не авторизованных изменений

Процент простоя в связи с инцидентами ИБ

Процент спама

Процент систем, защищенных антивирусом

Процент инцидентов ИБ

Процент ложных срабатываний

Повторные инциденты ИБ

Изменения устраняющие инциденты ИБ

Уровень сотрудников в сфере ИБ

Время между обнаружением и устранением

Механизмы улучшения:

- количество предложенных улучшений в отношении контролей и процедур;
- уменьшение количества несовпадений, обнаруженных в процессе тестирования и аудита.

Ключевые моменты процесса:

- Департамент Безопасности является владельцем процесса
- ИТ департамент управляет ИТ компонентами Информационной Безопасности

Информационная безопасность является неотъемлемой частью услуг и процессов ITSM, то есть увеличение количества услуг и процессов, в которых предусмотрены меры безопасности.

Управление Поставщиками (Supplier Management SUM)

Управление поставщиками (Supplier Management) – процесс, ответственный за обеспечение того, что договоры с поставщиками соответствуют требованиям бизнеса, и все поставщики выполняют свои контрактные обязательства. Процесс Управление поставщиками следит за тем, чтобы поставщики выполняли свои обязательства по контрактам – достигали целевых показателей в оговоренные сроки.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса взаимодействия с поставщиками
- Формирование процесса закупки, поставки, сопровождения и т.п. ИТ активов
- получение ценности за потраченные бизнесом деньги;
- обеспечение того, что все основополагающие контракты и соглашения с поставщиками соответствуют требованиям бизнеса, требованиям SLA и SLR;
- управление взаимоотношениями с поставщиками;

Важно понимать некоторые различия в терминологии. Так имеется две категории: сервис провайдер (Service Provider) и поставщик (supplier)

Провайдеры сервиса – организационная единица, предоставляющая тот или иной сервис. Различают:

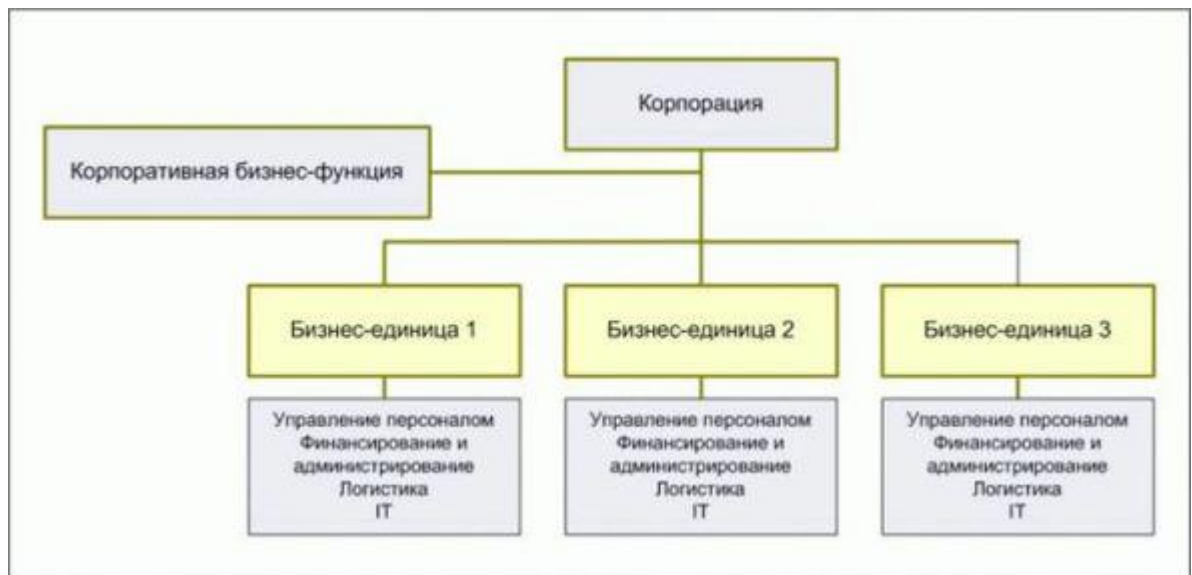
- Внутренний сервис провайдер – предоставляет сервис и включен в состав бизнеса. Как пример ИТ служба в компании.
- Совместный сервис провайдер – предоставляет сервисы различным бизнес юнитам. Как пример ИТ департамент компании.
- Внешний сервис провайдер – предоставляет сервисы различным клиентам. Как пример интернет провайдер.

Поставщик (Supplier) – третья сторона, ответственная за поставку товаров или услуг, необходимых для предоставления ИТ-услуг.

Понятия в некоторой степени пересекаются и как пример внешний сервис провайдер может являться поставщиком ИТ услуги для компании.

Типы поставщиков ИТ услуг можно условно разбить на три категории:

ТИП 1 – Бизнес Единица (Business Unit BU) – сегмент бизнеса, который имеет свои собственные метрики, планы, доходы и расходы. Каждая бизнес-единица владеет и управляет активами, которые использует для создания товаров и услуг с определенной ценностью.



Основной целью поставщиков услуг первого типа является обеспечение функциональной целостности и эффективности бизнес-единицы, за которой они закреплены. Другими словами, они предоставляют ИТ-услуги для удовлетворения узкого круга потребностей бизнеса. Основным недостатком является:

- фактически, развитие поставщика услуг ограничено возможным развитием бизнес-единицы, за которой он закреплен.
- решения принимает руководство организации, также является своего рода недостатком, так как зачастую оно не разбирается в технических тонкостях ИТ-области.

Из плюсов:

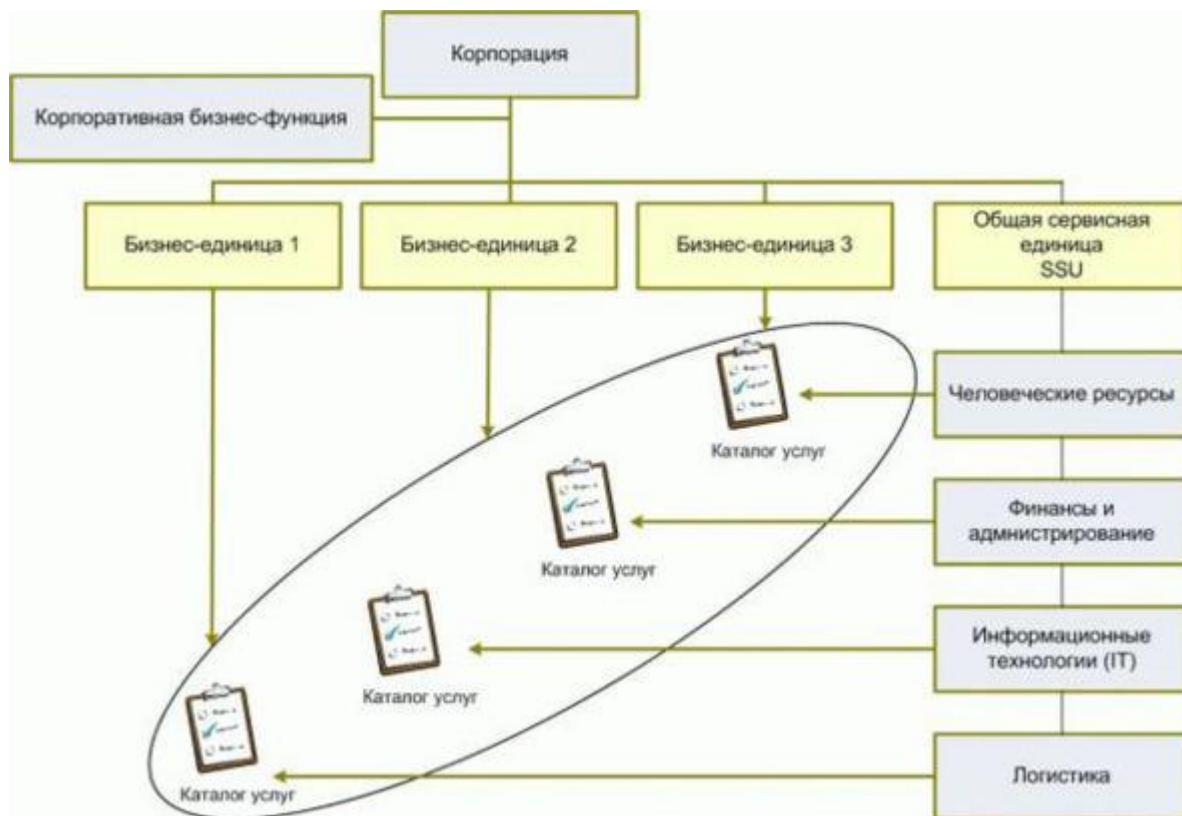
- бизнес не сталкивается с проблемами, возникающими во время взаимодействия с внешними поставщиками услуг.
- не сталкивается со сложностями свободного рынка.

Ввиду перечисленных особенностей поставщики услуг первого типа больше подходят для бизнеса, где ИТ лежит в основе конкурентного преимущества, и, следовательно, требует тщательного контроля непосредственно со стороны руководства организации.

ТИП 2 – Общий Поставщик Услуг (Service Shared Unit SSU) – объединение деловых функций, такие как финансовое управление, ИТ, управление персоналом и логистика, которые не всегда являются основой конкурентного преимущества. Отсюда руководителю организации и топ-менеджерам не обязательно контролировать и управлять ими.

Преимущества:

- Возможность создавать, развивать и поддерживать внутренний рынок сбыта своих услуг аналогично поставщикам, которые работают на свободном рынке.
- использование возможности корпорации.
- получают преимущества от относительно закрытого рынка.



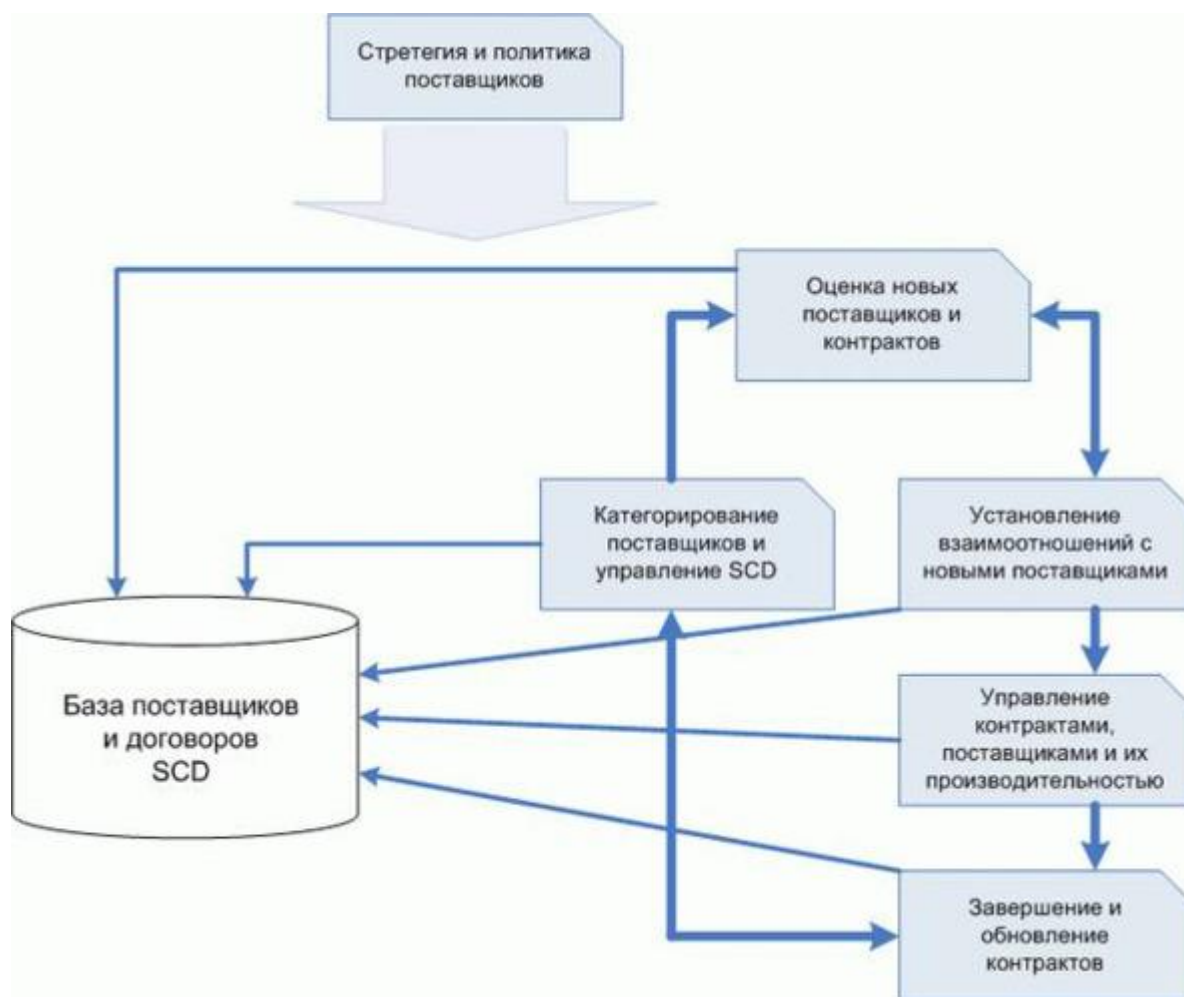
Тип 3 – Бизнес Единица (Business Unit) – Внешние поставщики услуг находятся вне организационной структуры своих заказчиков, в отличие от предыдущих двух типов. Поставщики услуг третьего типа обладают большим практическим опытом ввиду обслуживания различных заказчиков и областей рынка. Часто организации гораздо выгоднее обратиться к внешнему поставщику, чем владеть и управлять всеми активами, которые нужны для самостоятельной реализации услуги.

Деятельность по процессу Управления поставщиками включает в себя:

- формирование и соблюдение политики работы с поставщиками;
- формирование Базы поставщиков и договоров, управление ею;
- категоризация поставщиков и контрактов, оценка рисков;
- оценка и выбор поставщиков и контрактов;
- ведение переговоров и заключение контрактов и соглашений;
- Оценка новых поставщиков и контрактов

Центральным репозитарием для хранения информации является База поставщиков и договоров. База поставщиков и договоров (Supplier and Contract Database или SCD) – база данных или структурированный документ, используемый для управления договорами поставщиков на протяжении всего их жизненного цикла. SCD содержит ключевые атрибуты всех договоров с поставщиками. SCD должна включать следующее:

- категорирование поставщиков
- поиск и оценка новых поставщиков
- установление взаимоотношений с новыми поставщиками
- управление контрактами
- обновление и завершение контрактов



Оценка новых поставщиков и контрактов

При выборе поставщиков услуг необходимо учитывать множество факторов, в частности предыдущие достижения и текущие возможности поставщика, а также отзывы о нем других организаций. Более того, в зависимости от типа взаимоотношений с поставщиками, может появиться множество других ключевых факторов для выбора.

Услуга может поддерживаться одним или несколькими поставщиками. При этом многие отношения с поставщиками могут характеризоваться как партнерские. То есть в настоящее время организации отходят от традиционного иерархического построения отношений с поставщиками, в которых поставщики всегда зависели от своих заказчиков. Отношения с поставщиками характеризуются следующим:

- ориентация на стратегию – отношения выстраиваются в соответствии с культурой, ценностями и целями бизнеса, то есть в соответствии с его стратегией;
- интеграция – тесная интеграция процессов двух организаций;
- информационный поток – хорошо налаженный обмен информацией между процессами двух организаций;
- взаимное доверие – взаимное доверие между организациями;
- открытость – открытость в отношении производительности услуг, затрат и анализа рисков;
- коллективная ответственность – команды, объединяющие сотрудников двух организаций, несут ответственность за текущую производительность и развитие сотрудничества в будущем;
- общие риски и премии – соглашение о том, как будут распределены выгоды и сопутствующие риски.

Подход к выбору поставщиков должен быть формализован. Он должен быть основан на таких факторах как значение услуги, предоставляемой поставщиком, риски и стоимость.

Обязательным является проведение Анализа рисков перед заключением какого-либо соглашения. Анализ рисков должен рассмотреть все возможные риски: финансовые, потери репутации, операционные, правовые и т. п.

Обязательные части базового контракта:

- основные условия и сроки – срок, на который заключается контракт, стороны, которые его заключают, охват, определения и коммерческий базис;

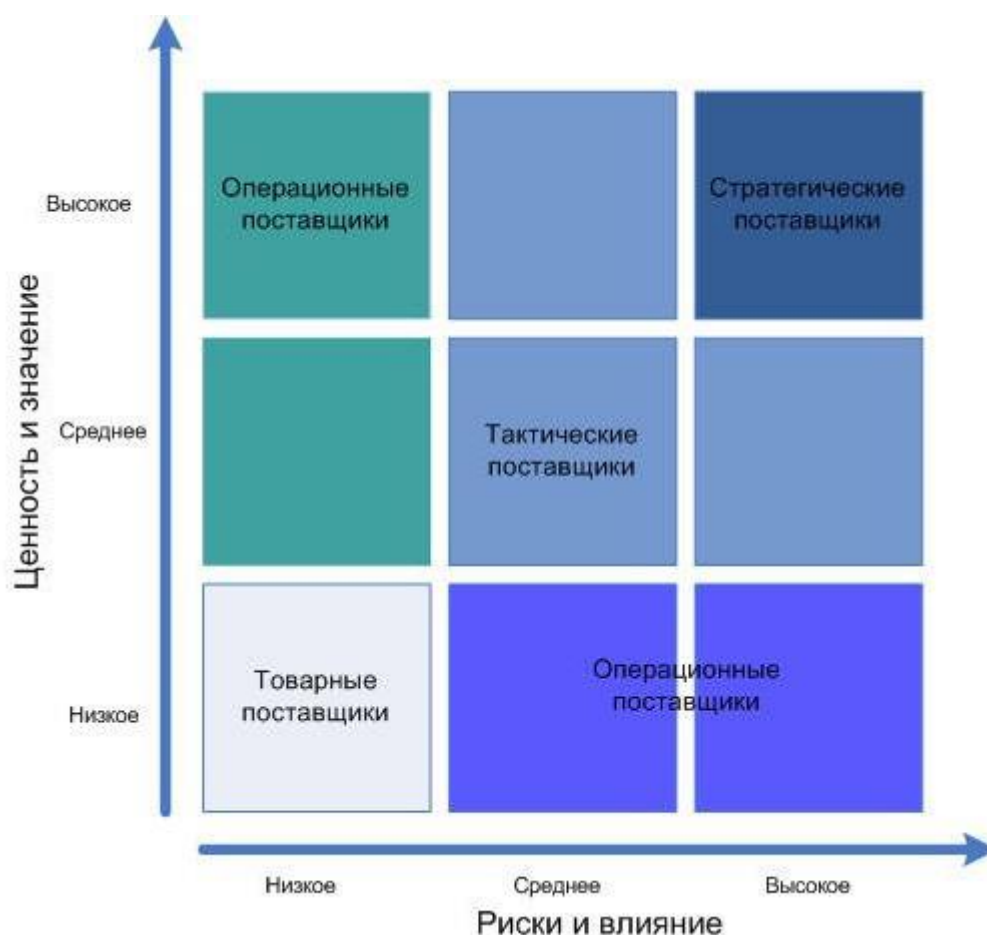
- описание услуг – функциональность, предоставляемая услугами, их производительность, доступность, безопасность и т. п., а также ограничения, влияющие на производительность услуг и их предоставление;

- нормы для услуг – метрики и способы измерения услуг, минимальные уровни производительности и качества. Обозначенные уровни должны быть четкими, достижимыми и измеряемыми, соответствовать приоритетам бизнеса и поддерживать целевые уровни SLA и SLR;

- производственная нагрузка – объемы производства, к которым применимы нормы для услуг и отдельные границы ценового диапазона;

- управленческая информация – информация, которую должен предоставить поставщик об операционной производительности. Необходимо, чтобы взаимоотношения строились на наиболее значимых метриках производительности услуг;

- ответственности и зависимости – описание обязанностей организации и поставщика.



Категорирование поставщиков и управление SCD

Процесс управления поставщиками должен быть адаптивным и уделять больше времени и внимания наиболее важным для организации поставщикам. Для этого необходимо расставить

приоритеты между поставщиками, то есть категорировать их. Лучше всего при этом оценить вклад поставщика, предоставляемую им ценность для бизнеса и риски, которые к нему относятся.

В соответствии с этим можно предложить следующие категории:

- стратегические поставщики
- тактические поставщики
- операционные поставщики
- товарные поставщики

Стратегические поставщики – взаимоотношения с такими поставщиками управляются на уровне руководства организации. Формируются долгосрочные контракты, и происходит обмен конфиденциальной информацией.

Тактические поставщики – взаимоотношения с такими поставщиками управляются на уровне менеджеров среднего звена. К тактическим поставщикам относятся те, кто вносит значимый коммерческий вклад и имеет тесные связи с бизнесом.

Операционные поставщики – поставщики, предоставляющие операционные услуги и продукты. Взаимоотношения с такими поставщиками управляются менеджерами нижнего уровня и включают в себя нечастые, но регулярные контакты и обзоры производительности.

Товарные поставщики – поставщики, предоставляющие продукты с низкой ценностью или поставщики, услуги и продукты которых могут быть легко заменены альтернативами, предлагаемыми другими участниками рынка.

Входами процесса Управления поставщиками являются:

- информация от бизнеса – стратегии, планы, бюджет бизнеса, а также его текущие и будущие требования;
- стратегии и планы поставщиков
- информация о производительности поставщиков
- финансовая информация
- информация об услугах

Выходами процесса Управления поставщиками являются:

- отчеты о производительности поставщиков и контрактов – эта информация используется на обзорных встречах для отображения качества услуг, предоставляемых поставщиками и контрактами;

Участники процесса:

- Менеджер по поставкам

Ключевые моменты процесса:

- Наличие Базы Данных Поставщиков и Контрактов (Suppliers and Contracts Database)
- Департамент Снабжения и логистики является владельцем процесса

В качестве ключевых показателей эффективности могут выступать:

- защищенность бизнеса от плохой производительности поставщиков или сбоев в обеспечении;
- увеличение количества поставщиков, выполняющих требования контрактов;

- уменьшение количества нарушений контрактов;

Доверит ли заказчик определенную деловую активность внешним поставщикам или внутренним, зависит от ответа на следующие вопросы:

- Требуется ли деловая активность специфических активов?
- Как часто используется деловая активность в бизнес-цикле?
- Насколько сложна деловая активность?
- Сложно ли определить высокий уровень производительности?
- Сложно ли измерить уровень производительности?
- Насколько тесно она связана с другими активностями и активами бизнеса?
- Ее отделение вызовет много проблем и увеличит сложность бизнес-процессов?

В зависимости от ответов на эти вопросы заказчики выбирают тип поставщика услуг.

Основными рисками для Управления поставщиками являются недостаточность информации, плохо налаженный обмен информацией между поставщиками и бизнесом, некорректные или невыполнимые цели, нехватка ресурсов и финансового обеспечения.

ЭТАП ВНЕДРЕНИЯ (Transition Stage)

Введение

Цели этапа Внедрения:

- Проектирование новых и изменение имеющихся сервисов для организации
- Формирование процесса передачи сервиса в эксплуатацию.
- Гарантирование что сервис может быть управляем,
- Эффективное планирование и управление потоком изменений
- Гарантирование что сервис соответствует бизнес требованиям,
- Гарантирование что сервис сопровождается и поддерживается на должном уровне
- Гарантирование что сервис соответствует требованиям Пакет Сервис Дизайна (Service Design Package SDP).
- Передача сервиса в «рабочую» среду
- планирование/управление мощностями и ресурсами для комплектования, сборки, тестирования и запуска в промышленную эксплуатацию услуг, а также обеспечение функционирования услуг в соответствии с требованиями инвесторов и заказчиков;
- построение точной и последовательной системы оценки мощности услуг и формирование перечня рисков прежде, чем новая или измененная услуга будет выпущена в промышленную эксплуатацию;
- формирование набора активов услуг и конфигураций, которые попадают на этап Внедрения, и управление ими;
- предоставление информации, необходимой для принятия решений о введении услуги в промышленную эксплуатацию после тестирования;
- предоставление эффективных и повторяемых механизмов для сборки и инсталляции, которые могут быть использованы для развертывания релизов в среде промышленной эксплуатации и среде тестирования;
- обеспечение управления, поддержки и корректной эксплуатации услуг в соответствии с требованиями, определенными на этапе Проектирования.
- планирование ресурсов и мощностей, необходимых для комплектования, сборки, тестирования, публикации, развертывания и вывода новых или измененных услуг в промышленную эксплуатацию;
- предоставление поддержки для персонала в рамках Внедрения;
- планирование изменений, необходимых для эффективного управления активами заказчиков, активами услуг и конфигурациями;

- ведение отчетности обо всех проблемах, рисках и расхождениях перед заинтересованными сторонами и теми, кто ответственен за принятие решений;
- координация проектов, поставщиков и контрактов, поддерживающих услуги.

Задачами этапа Внедрения являются:

- определить ожидания заказчиков относительно того, как новая или измененная услуга поможет их бизнесу;
- помочь в интеграции новой или измененной услуги в бизнес-процессы заказчиков;
- уменьшить разницу между прогнозируемой и реальной производительностью;
- уменьшить количество известных ошибок и рисков на этапе запуска новой или измененной услуги в промышленную эксплуатацию;
- обеспечить то, что услугу можно будет использовать в соответствии с установленными для нее требованиями и ограничениями.

Этап Внедрения предоставляет ценность для бизнеса тем, что:

- улучшает способность адаптироваться к новым требованиям или обстоятельствам на рынке;
- улучшает управление на уровне внедрения в рамках поглощений, разъединений компаний, приобретения или перемещения услуг;
- увеличивает количество успешных для бизнеса изменений и релизов;
- улучшает точность прогнозирования относительно уровня и качества новых или измененных услуг;
- улучшает согласованность с требованиями бизнеса и руководства;
- уменьшает количество расхождений между утвержденными бюджетами/планами и реальностью;
- увеличивает продуктивность персонала вследствие улучшения планирования и использования новых или измененных услуг;
- уменьшает случаи временной приостановки или изменения контрактов на программное и аппаратное обеспечение вследствие соединения или разъединения компонентов;
- улучшает понимание уровня риска во время изменения и после него.

Данный этап определяется следующими процессами (7):

- Управление процессом передачи сервиса и поддержка
- Управление процессом изменений
- Управление ИТ активами и конфигурацией
- Управление релизами и внедрением
- Управление тестированием и внедрением
- Оценка изменений
- Управление базой знаний

Входы, поступающие с этапа Построения стратегии, влияют на подход, структуры и ограничения этапа Внедрения:

- Портфель услуг;
- Портфель заказчиков – база данных или структурированный документ, используемый для хранения информации обо всех Заказчиках поставщика услуг;
- Портфель договоров – база данных или структурированный документ, используемый для управления договорами на оказание услуг или Соглашениями между поставщиками услуг и их заказчиками;
- модель жизненного цикла услуги;
- политики;
- стратегии;
- ограничения;
- архитектуры;
- требования к Внедрению;
- План управления услугами.

Этап Проектирования услуг является источником триггеров или механизмов запуска для этапа Внедрения. В первую очередь это проектная документация (SDP), которую необходимо реализовать. Она включает в себя следующие компоненты:

- определение услуги;
- структура услуги;
- финансовая модель и модель затрат;
- модель мощностей/ресурсов;
- модель интеграции процесса Управления услугами;
- модель эксплуатации услуги;
- спецификация дизайна и интерфейса;
- дизайн релиза;
- критерии приемки;
- Запросы на изменения (RFC).

Этап Непрерывного улучшения услуг предоставляет на вход этапа Внедрения информацию в терминах предлагаемых улучшений политик, практик и процессов внедрения.

Этап Эксплуатации предоставит на вход этапа Внедрения информацию для тестирования и приемки услуг в терминах достижения услугами требуемых показателей.

Выходами этапа Внедрения являются:

- утвержденная документация для релиза и развертывания услуг;
- обновленный Пакет Услуг. Пакет услуг (Service Package) – детализированное описание услуги, доступной для предоставления заказчикам;
- обновленные Каталог услуг и Портфель услуг;
- документация для внедряемых или списываемых услуг.

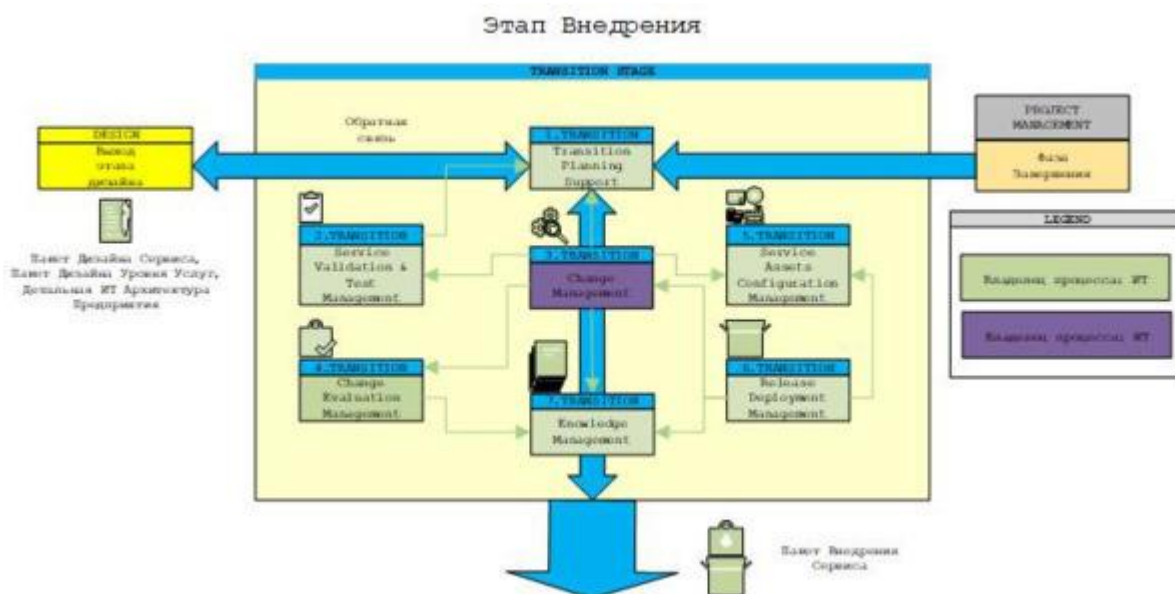
Можно выделить два типа процессов этапа Внедрения:

Процессы, поддерживающие жизненный цикл услуги:

- Управление изменениями;
- Оценка услуг и Управление конфигурациями;
- Управление знаниями.

Процессы в рамках Внедрения:

- Планирование и поддержка Внедрения;
- Управление релизами и развертыванием;
- Тестирование и подтверждение услуг;
- Оценка.



Планирование Внедрения и Поддержки (Transition Planning & Support TPS)

Процесс Планирования Внедрения и Поддержки сервиса является частью этапа «Внедрения». Данный процесс отвечает на такие вопросы как:

- Формирование процесса внедрения сервиса.
- Формирование процесса поддержки сервиса.

Деятельность по процессу:

- Утверждение процесса Внедрения и Поддержки сервисов
- учет операционных требований и требований проектирования в планах Внедрения;
- управление деятельностью в рамках Внедрения;
- управление процессами, рисками и расхождениями в рамках Внедрения;
- взаимодействие с заказчиками, пользователями и другими заинтересованными сторонами в вопросах, касающихся внедрения;
- мониторинг и улучшение производительности Внедрения как процесса.
- Формирование стратегии внедрения
- Определяет план внедрения и распределение ресурсов
- Проверка и принятие SDP, Service Acceptance Criteria and evaluation report

Внедрение требует внимательного подхода и последовательных действий.

Первое, что необходимо определить – **Стратегия Внедрения**. Она определяет общий подход организации к внедрению и должна рассматривать следующее:

Цели Внедрения;

- контекст внедрения (заказчики, договора и т. п.);
- охват – то, что входит и не входит в рамки Внедрения;
- применяемые стандарты, соглашения, требования регуляторов и контрактов;
- организации и инвесторы, вовлеченные во Внедрение;

Структура Внедрения:

- применяемые политики, процессы и практики;
- роли и ответственности;
- распределение ресурсов в рамках Внедрения;
- формирование требований к подготовке и обучению;
- механизм авторизации для доступа к релизам и изменениям;
- использование накопленного опыта, практики и данных;
- распределенные ресурсы и услуги, поддерживающие Внедрение;
- критерии успеха для каждой стадии Внедрения, а также остановки или перезапуска деятельности в рамках Внедрения;
- определение требований и содержания новой или измененной услуги в контексте Внедрения;
- персонал – назначение на роли, обучение и т. п.;

Второй стадией является **подготовка к Внедрению**. На этой стадии проверяются и собираются все входы процессов, наличие необходимых конфигураций и общая готовность к Внедрению. В частности, детально рассматривается проектная документация (SDP), поступившая с этапа Проектирования. Именно она во многом определяет Внедрение.

Подход к Внедрению:

- Модель Внедрения;
- планы управления изменениями, активами, конфигурациями и знаниями;
- планирование затрат, ресурсов и оценочных работ;
- подготовка к Внедрению;
- оценка;
- комплектование, сборка, развертывание и ранняя поддержка релиза;
- контроль и управление проблемами, ошибками, инцидентами и т. п.

- мониторинг процессов и формирование отчетности;
- система измерения производительности услуг;
- ключевые показатели производительности и цели по улучшению.
- выходы деятельности в рамках Внедрения, в том числе документация.

Следующая стадия – **планирование и координация Внедрения**. План Внедрения описывает задачи и действия, необходимые для передачи релиза на тестирование или промышленную эксплуатацию. Одним из основных вопросов является распределение ресурсов для конкретных деятельности в рамках Внедрения.

Набор планов внедрения находится между Стратегией внедрения и планами низших уровней – планами релизов, сборки, тестирования и т. п.

Далее необходимо обеспечить поддержку Внедрения. Сюда относятся вопросы взаимодействия со всеми заинтересованными лицами, мониторинга производительности услуг и обеспечение обратной связи с другими этапами жизненного цикла. Формирование отчетности о ходе процессов и доведение ее до руководства и заинтересованных лиц позволит сделать выводы о соответствии планам, стратегиям и стандартам, а также эффективности Внедрения в целом.

Входы процесса:

Процесс Управление Дизайном сервисов
 Процесс Управления Требованиями
 Процесс Управления Доступностью
 ИТ архитектура
 RFC
 CMDB
 CMS
 SKMS
 Рекомендации CAB
 SLAM отчеты

Выходы процесса:

Подписанный протокол решения ИТ комитета
 Политики
 Процедуры
 Service Provider Interfaces SPIs
 Роли и ответственности
 Оценка планирования ресурсов по внедрению
 Подготовка к внедрению
 Формирование требований по обучению
 Авторизация изменений и релизов
 Стратегия Внедрения
 Набор планов Внедрения.

Участники процесса:

ИТ комитет
 ИТ архитектор
 Руководители ИТ подразделений
 Экспертная группа
 Проектная группа
 Service Transition Manager
 Early Life Support

Ключевые показатели производительности процесса:

- количество релизов, которые соответствуют согласованным требованиям заказчиков по затратам, качеству, охвату и временным рамкам;

- уменьшение несоответствия между тем, что получается на практике, и тем, что планировалось;
- увеличение удовлетворенности пользователей и заказчиков планами и коммуникациями, которые позволяют настраивать бизнес-деятельность в соответствии с планами Внедрения;
- уменьшение количества рисков, вопросов и задержек, вызванных некорректным планированием.

Управление Изменениями (Change Management CHM)

Процесс Управления Изменениями является частью этапа «Внедрения». Данный процесс отвечает на такие вопросы как:

- Формирование процесса управления изменениями.
- Кто ИНИЦИИРУЕТ (RAISED) запрос на изменения
- Какова ПРИЧИНА (REASON) запроса на изменения
- Какова ОТДАЧА (RETURN) требуется от запроса на изменения
- Какие РИСКИ (RISKS) влечет в себе запрос на изменения
- Какие РЕСУРСЫ (RESOURCES) требует выполнения запроса на изменения
- Кто ОТВЕТСТВЕННЫЙ (RESPONSIBLE) за создание, тестирование и выполнения запроса на изменения
- Какова СВЯЗЬ (RELATIONSHIP) между этим запросом на изменения и другими

Цели процесса:

- использования стандартных методов и процедур для быстрой и эффективной реализации изменений;
- фиксации всех изменений в активах услуг и конфигурациях в Системе Управления конфигурациями (CMS);
- оптимизации всех рисков для бизнеса.

Управление изменениями представляет ценность для бизнеса тем, что:

- категоризирует цели изменений бизнеса и заказчиков и помогает их осуществить;
- реализует изменения, которые соответствуют потребностям заказчиков, одновременно с оптимизацией затрат;
- старается выполнять требования закона, контрактов, руководства и регуляторов;
- уменьшает количество неудавшихся изменений и, соответственно, количество сбоев, остановок и простоев услуг;
- осуществляет изменения в установленном бизнесом временном интервале;
- следит за изменениями на всем жизненном цикле услуг;
- старается обеспечить лучшие показатели в аспектах качества, времени и затрат;
- оценивает риски, сопутствующие внедрению;
- помогает увеличить продуктивность работы персонала тем, что минимизирует нарушения и сбои, а, следовательно, улучшает доступность услуг;
- уменьшает Среднее время восстановления услуг (MTRS) посредством быстрой и успешной реализации изменений;
- сотрудничает с процессом изменения бизнеса для выявления возможностей улучшения бизнеса.

Хорошо структурированные и запланированные изменения помогают бизнесу сократить издержки и повысить эффективность.

Модель процесса изменения должна включать следующее:

- шаги, которые должны быть предприняты для реализации изменения, в том числе разрешение проблем и непредвиденных событий;
- хронологический порядок шагов;
- ответственности и распределение обязанностей;
- границы, в том числе временные, каждой деятельности в рамках процесса;

Ни одно изменение не должно осуществляться без четкого планирования действий в случае, если оно будет неудачным – «планирование исправления». В идеале должен быть некий план «backup», который позволит организации вернуться в состояние, предшествующее изменению. Только посредством оценки того, какие действия по исправлению возможны в конкретной ситуации, можно определить риски, соответствующие изменению.

Деятельность в рамках процесса Управления изменениями включают:

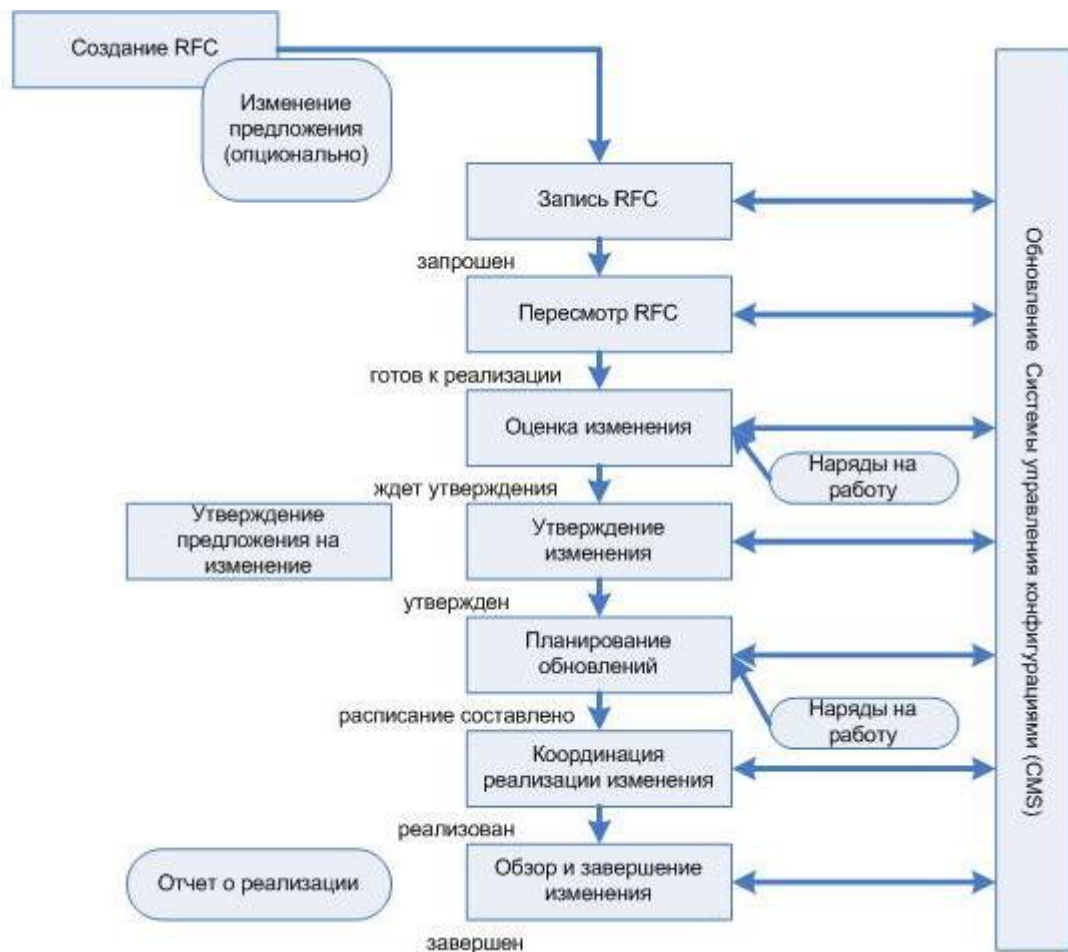
- планирование и контроль изменений;
- составление расписаний для изменений и релизов;
- обеспечение коммуникации между всеми участниками и компонентами;
- авторизация к изменениям (то есть разрешения доступа тем, кто уполномочен вносить изменения) и принятие решений относительно изменений;
- формирование планов по исправлению, которые будут задействованы в случае неудачных изменений;
- измерение и контроль;
- формирование управленческой отчетности;
- оценка влияния изменения;
- непрерывное улучшение.
- Утверждение процесса Управления Изменениями
- Формирование комитета по Управлению Изменениями
- Формирование списка «пред-утвержденных» изменений
- Изменение Уровня Предоставления Сервисов (Service Level Agreement SLA)
- Принятие решения по выводу ИТ сервиса из сопровождения



Стандартные действия при реализации отдельных изменений:

- создание Запроса на изменение (RFC);
- пересмотр и проверка RFC, фильтрация изменений;
- оценка и определение изменения;
- установить уровень управления изменением;
- определить участников процесса;
- оценить мотивацию бизнеса, издержки, риски и выгоды, связанные с изменением;
- запросить независимую оценку изменения.
- утверждение изменения (в том числе определение механизмов авторизации к нему);

- формирование планов обновлений;
- координация реализации изменения;
- обзор и завершение изменения.



При внедрении процесса управления изменениями необходимо определить следующие важные атрибуты:

Определить, по возможности *категоризацию воздействия* с указанием метрик:

- Высокое (High) воздействие – Изменение воздействует на всех пользователей или критичен для бизнеса или Изменение затрагивает критические компоненты сервиса
- Среднее (Medium) воздействие – Изменение воздействует на (значительную или нет) группу пользователей или бизнеса, или Изменение затрагивает критические, но зарезервированные компоненты сервиса
- Низкое (Low) воздействие – Изменение воздействует на одного пользователей или не критичен для бизнеса, или Изменение затрагивает не критические или второстепенные компоненты сервиса

Категоризацию срочности с указанием метрик:

- Высокая (High) срочность – Изменение требует немедленного вмешательства или выполнения
- Средняя (Medium) срочность – Изменение требует вмешательства, но время разрешения в пределах SLA
- Низкая (Low) срочность – Изменение не требует немедленного вмешательства

Определить, по возможности *уровень риска*, при применении и не применении данных изменений:

- Высокий (High) риск воздействие
- Среднее (Medium) риск воздействие
- Низкое (Low) риск воздействие
- Воздействие не определённо (Not assessed)

Порядок реагирования для каждой категории изменений:

•Время выполнения изменений – максимальное время, в течении которого ИТ департамент обязуется выполнить изменения.

Определение *источников поступления изменений*:

- Запросы на изменения со стороны бизнеса (Процессы управления доступностью, требованиями)
- Запросы на изменения со стороны департамента Безопасности
- Анализ инцидентов (Процесс управления инцидентами)
- Анализ запросов (Процесс управления запросами)
- Анализ проблем (Процесс управления проблемами)
- Мониторинг событий и логов (Процесс управления Событиями)
- Анализ релизов (Процесс управления Релизами)
- Запросы на изменения со стороны ИТ департамента (Этап Улучшения Сервиса)



Статусы изменений:

- Инициирован (Initiate)
- Одобрённый (Approved)
- Активный (In progress)
- В ожидании (On pending)
- Приостановлённый (On hold)
- Проверённый (Validated and Reviewed)
- Выполнённый (Completed)

- Закрытый (Closed)
- Активность проигнорирована (skipped)

Классификация изменений по типам и подтипам (зависит от специфики организации, предпочтениям и т п):

- Стратегические изменения
- Тактические изменения
- Оперативные изменения
- Стандартные изменения
- Стандартные «пред-утвержденные» изменения
- Экстренные изменения
- Не классифицированные изменения
- «Стандартизированные» изменения
- Заранее «одобренные» Изменения

Impact	High	3	2	1
	Medium	4 (Standard Change)	3	2
	Low	Candidate for Automation	4 (Standard Change)	3
		Low	Medium	High
		Probability		

Определение групп выполнения и подтверждения изменений. Зависит от организационной структуры ИТ департамента, классификации изменений и т п:

- Оператор центра Поддержки Пользователей
- Группы подтверждения изменений (по процессам)
- Комитет по утверждению изменений
- Менеджер по управлению изменениями
- Первая линия поддержки
- Вторая линия поддержки
- Третья линия поддержки
- Четвертая линия – поддержка производителя

Результаты выполнения изменений:

- Удално выполненный (Successfully implemented)
- Выполненный с незначительными проблемами (Implemented with Issues)
- Частично выполненный (Partially implemented)
- Не выполненный (Failed)
- Отказанный (Rejected)
- Отозванный (Cancelled)
- Не одобренный (Unauthorized)

Определение типовых под-процессов (шаблонов) для различных изменений

Определение метрик и показателей оценки эффективности и результативности процесса

Кроме элементов, выше указанных, необходимо также определить следующие элементы:

• порядок информирования пользователя, сотрудника ИТ и менеджера проекта или супервайзера на различных этапах жизни изменений.

- Метрики соглашений
- План внедрения изменений (Implementation Plan)
- Оценка рисков при внедрении или не внедрении изменений (Risk Assessment Plan)
- План тестирования изменений (Test Plan)
- План отката изменений (Back out Plan)

В процессе управления изменениями анализируется возможность и формируется список «заранее одобренных» изменений или изменений, которые можно автоматизировать. В процессе анализа используются основные атрибуты:

- Воздействие изменений
- Вероятность возникновения
- Простота и ясность операций

Входами процесса Управления изменениями являются:

Политики и стратегии изменений и релизов;

Запросы на изменения;

Предложение изменения;

Планы изменения, внедрения, релиза, развертывания, тестирования, оценки и исправления;

График изменений и Ожидаемый простой услуги (PSO);

активы и конфигурационные единицы;

результаты и отчеты тестирования/оценки.

Выходами процесса Управления изменениями являются:

Подписанный протокол решения ИТ комитета

отклоненные RFC;

утвержденные RFC;

изменения услуг и инфраструктуры – результат утвержденных RFC;

новые, измененные или распределенные активы, или конфигурационные единицы;

график изменений;

пересмотренный Ожидаемый простой услуги (PSO);

утвержденные планы изменений;

решения и действия по реализации изменений;
документация и записи изменений;
отчеты Управления изменениями.

Участники процесса:

ИТ комитет

Комитет по Управлению Изменениями (Change Advisory Board CAB)

Комитет по Управлению Экстренными Изменениями (Emergency Change Advisory Board ECAB)

Ключевые показатели производительности для Управления изменениями должны быть связаны с целями бизнеса, в частности, отражать сокращение издержек, увеличение доступности и надежности услуг, которые стали возможными в результате реализованных изменений. Такими показателями могут быть:

- количество реализованных изменений, которые смогли удовлетворить согласованные требования заказчиков в качестве/издержках/времени;
- выгода изменений – сравнение «ценность сделанных улучшений “+” предотвращенное негативное влияние» и стоимости реализации изменений;
- уменьшение количества сбоев услуг, дефектов и дополнительных работ;
- уменьшение количества неутвержденных изменений;
- уменьшение количества невыполненных запросов на изменение;
- уменьшение количества незапланированных изменений и экстренных исправлений;
- процент успешных изменений – отношение изменений, признанных успешными, к общему количеству утвержденных запросов на изменение;
- уменьшение количества изменений, в рамках которых есть работы по исправлению;
- уменьшение количества неудавшихся изменений;
- уменьшение количества инцидентов, связанных с изменениями;

Критерии эффективности – (KPI)

Количество изменений

Количество «стандартных» изменений

Количество срочных изменений

Количество важных изменений

Количество «не авторизованных» изменений

Отношение изменений к инцидентам

Количество изменений со статусом «overdue»

Количество изменений, выполненных в срок

Количество изменений со статусом «rejected»

Количество изменений, вызванных инцидентами

Количество изменений, вызванных запросами

Количество изменений, вызванных событиями

Количество изменений, вызванных проблемами

Средний срок закрытия изменений

Процесс управления изменениями один из наиболее важных и сложных процессов при построении системы управления ИТ сервисами, так как требует вовлеченность различных

подразделений организаций. Кроме этого, данный процесс используется как при предоставлении сервиса, так и при его сопровождении.

Управление ИТ активами и Конфигурациями (Assets & Configuration Management SACM)

Управление активами и конфигурациями (Service Asset and Configuration Management или SACM) – процесс, ответственный за Управление конфигурациями и Управление активами. Целью SACM является определение и контроль компонентов услуг и конфигурационных единиц, а также предоставление достоверной информации о состоянии услуг и инфраструктур. Процесс фактически осуществляет инвентаризацию активов и назначение ответственных за их контроль.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса
- Управление ИТ активами
- Управление конфигурациями

Деятельность по процессу:

- Процесс управления и планирования
- Идентификация компонентов
- Контроль конфигураций
- Отчет о состоянии
- Проверка и аудит состояния

Управление и планирование

Не существует единого шаблона для осуществления SACM. Менеджеры каждой организации устанавливают уровень Управления конфигурациями, приемлемый для конкретного случая и то, как его можно достичь. Это отображается в Плана управления конфигурациями.

Пример содержания **Плана управления активами и конфигурациями.**

Контекст и цель.

Охват:

- применяемые услуги;
- среда и инфраструктура;
- географическое месторасположение.

Требования:

- требования стратегии и политик;
- требования бизнеса, Управления услугами и контрактов;
- совокупность требований к подотчетности и трассируемой;
- требования Системы управления конфигурациями.

Применяемые политики и стандарты:

- политики;
- индустриальные стандарты;
- внутренние стандарты, относящиеся к Управлению конфигурациями, например, стандарты к оборудованию.

Организация Управлением конфигурациями:

- роли и ответственности;
- комитеты для контроля изменений и конфигураций;
- авторизация.

Процессы и процедуры в рамках Управления активами и конфигурациями:

- идентификация конфигураций;
- управление версиями;
- управление интерфейсами;

- управление поставщиками;
- управление изменениями конфигураций;
- релиз и развертывание;
- управление сборкой;
- управление снабжением;
- управление CMS.

Ссылка на План реализации

Управление и контроль необходимых связей и интерфейсов, в частности, с финансовым управлением активами и поставщиками.

Идентификация конфигураций

Для идентификации конфигураций важно:

- определить, как будут категорироваться активы и конфигурационные единицы;
- определить подход к идентификации и наименованию всех активов и конфигурационных единиц;
- определить роли и ответственности для владельцев конфигурационных единиц отдельных типов в рамках этапов жизненного цикла, например, владелец услуги в процессе релиза.

Деятельность в рамках идентификации конфигураций включает в себя:

- определение и документирование критериев выбора конфигурационных единиц и составляющих их компонентов;
- выбор конфигурационных единиц и их компонентов на основе установленных критериев;
- назначение уникальных идентификаторов для выбранных конфигурационных единиц;
- определение атрибутов для каждой конфигурационной единицы;
- определение для каждой конфигурационной единицы момента, когда она поступает в Управление конфигурациями;
- определение владельца, ответственного за каждую конфигурационную единицу.

Входы процесса:

Запросы на изменения (Change Requests)
Заказы на закупку (Purchase Orders)
Запрос на приобретение (Acquisition Requests)
Запрос на сервис (Service Requests)

Выходы процесса:

CMDB
Категории и классификация компонентов (CI)
Атрибуты компонентов
Связи компонентов
Предоставляет данные для всех процессов управления сервисами

Участники процесса:

ИТ архитектор
Руководители ИТ подразделений
Экспертная группа
Сотрудники ИТ департамента
Service Asset Manager
Configuration Manager
Configuration Analysis
Change Manager

Управление конфигурациями отвечает за то, чтобы отдельные компоненты услуги, системы или продукта, были должным образом определены, снабжены всем необходимым

и контролировались. Процесс также контролирует все изменения компонентов. Он предоставляет модель конфигураций со всеми связями между активами и конфигурациями. Объектом рассмотрения является Конфигурационная единица.

Конфигурационная единица (Configuration Item или CI) – любой компонент, который нуждается в управлении для того, чтобы предоставлять услугу. Информация о каждой КЕ регистрируется в форме Записи о КЕ в Системе управления конфигурациями и поддерживается актуальной в течение всего жизненного цикла процессом Управления конфигурациями. КЕ находятся под контролем Управления изменениями. Типичными примерами являются услуги, оборудование, программное обеспечение, здания, люди и документы, такие как Процессная документация и Соглашения об уровне услуг (SLA).

Для того чтобы управлять конфигурационными единицами, их нужно определить и классифицировать. ITIL рекомендует следующие категории:

- Конфигурационная Единица жизненного цикла
- Конфигурационная Единица услуги
- Конфигурационная Единица организации
- Внутренние Конфигурационные Единицы
- Внешние Конфигурационные Единицы
- Конфигурационная Единица интерфейса

Конфигурационная Единица жизненного цикла – бизнес-кейс, планы сервис-менеджмента, проектная документация, планы релизов, изменений и тестирования. Эти конфигурационные единицы предоставляют полную картину об услугах поставщика и их предоставлении, ожидаемых выгод от использования, затратах и сроках релиза.

Конфигурационная Единица услуг:

- возможности услуг – управление, организация, процессы, знания, люди;
- ресурсы услуг – капитал, системы, приложения, информация, данные, инфраструктуры и т. п.;
- модель услуг;
- пакет услуг;
- пакет релизов;
- критерии приемки услуг.

Конфигурационная Единица организации. Некоторая документация определяет характеристики CI, некоторая сама является CI и требует контроля, например, стратегия бизнеса или политика организации;

Внутренняя Конфигурационная Единица – материальные и нематериальные активы, которые необходимы для предоставления и управления услугами;

Внешняя Конфигурационная Единица – требования заказчиков, соглашения, релизы поставщиков и внешние услуги;

Конфигурационная Единица интерфейсов – активы, необходимые для предоставления услуг «от начала до конца» в рамках Интерфейса поставщика услуг. Интерфейс поставщика услуг (Service Provider Interface или SPI) – интерфейс между поставщиком услуг и пользователем, заказчиком, бизнес-процессом, или поставщиком. Анализ интерфейсов поставщика услуг помогает координировать сквозное управление услугами.

Для управления совокупностью активов Управление активами и конфигурациями ведет Систему управления конфигурациями.

Система управления конфигурациями (Configuration Management System или CMS) – набор инструментов и баз данных, которые используются для управления данными о конфигурациях поставщиком услуг. CMS включает в себя инструменты для сбора, хранения, управления, обновления и представления информации обо всех конфигурационных единицах и их взаимоотношениях.

Модель конфигураций должна включать в себя связи и позицию каждой конфигурационной единицы. Важной частью Управления конфигурацией является определение уровня контроля для каждой конфигурационной единицы. Для этого применяется иерархический подход, так как

каждая CI может являться частью другой CI или группы CI. Например, база данных может использоваться многими приложениями. Конфигурационные единицы нижних уровней не подвержены детальному контролю и аудиту. Например, клавиатуры, используемые в организации, могут послужить примером CI нижнего уровня. Важно отметить, что в зависимости от конкретной организации, критерии выбора CI нижнего уровня отличаются. Всем конфигурационным единицам необходимо назначить имена, состоящие из идентификатора и версии. Имена должны быть уникальными. Помимо этого, все физическое оборудование должно иметь бирки, по которым их можно будет легко идентифицировать.

Атрибуты конфигурационных единиц описывают характеристики, значимые в рамках SACM. В базе данных должны содержаться атрибуты каждой конфигурационной единицы. ITIL выделяет следующие стандартные атрибуты:

- уникальный идентификатор;
- тип CI;
- имя/описание;
- версия;
- расположение;
- дата поставки;
- детали лицензии (в частности, дата ее истечения);
- владелец/куратор;
- статус;
- поставщик/источник;
- документация;
- данные истории, например, аудиторские отчеты;
- тип связей;
- соответствующий SLA.

Чаще всего характеристики CI содержатся в документации к ней. Связи конфигурационных единиц отражают то, как они взаимодействуют друг с другом в процессе предоставления услуг. Информация о связях хранится в CMS.

Основные связи между CI:

- CI является частью другой CI. Например, сервер является частью инфраструктуры сайта. Это отношение «родитель-ребенок»;
- CI соединен с другим CI. Например, персональный компьютер соединен с локальной сетью;
- CI использует другой CI. Например, программа использует модуль другой программы;
- CI установлена на другую CI, например, Microsoft Excel на персональный компьютер.
- CI может иметь множество связей. Например, быть частью другой CI и одновременно использоваться другими CI.

Контроль конфигураций предоставляет механизмы контроля для конфигураций. CI не может быть перемещена, изменена, удалена без соответствующего контроля. Процедуры и политики контроля включают в себя:

• лицензионный контроль – проверяет количество людей, которые используют лицензионный продукт, следит за тем, чтобы в организации не использовались нелегальные продукты, следит за сроками истечения лицензий и т. п.;

- управление изменениями;
- контроль версий активов, программного и аппаратного обеспечения, релизов, сборок и т. п.;
- контроль активов – возможности, место хранения, CMS;
- контроль сборки с использованием документации от CMS;
- поддержка и миграция электронных данных и информации;
- формирование базы активов и конфигурационных единиц перед релизом;
- контроль развертывания;
- установка;
- управление целостностью Библиотеки эталонного ПО.

Библиотека эталонного ПО (Definitive Media Library (DML)) – одно или несколько защищенных хранилищ, в которых находятся определенные и авторизованные версии всех конфигурационных единиц, относящиеся к программному обеспечению. Также может содержать CI, ассоциированные с ПО, такие как лицензии и документация.

Механизмы контроля должны быть спроектированы и встроены в новую или измененную услугу на ранних этапах ее развертывания.

Каждая CI имеет ряд дискретных *статусов* в рамках своего жизненного цикла. Значимость каждого статуса определяется использованием CI в его рамках. Выделяют следующие статусы:

- разработка или проектирование – CI находится на этапе проектирования и пока ее нельзя использовать;
- утверждена – CI утверждена, и могут проводиться дальнейшие работы;
- отозвана – CI больше не используется.

Запись о конфигурации содержит следующие данные:

- информация о конфигурации – идентификационный номер, версия, статус, история изменений и т. п.);
- конфигурация услуги или продукта – статус проектирования или сборки;
- статус релиза обновления для конфигурации;
- изменения, которые осуществлены или осуществляются;
- сбор результатов тестирования качества.

Проверки

Включает в себя набор следующих проверок:

- соответствие документации и актуального состояния CI;
- физическое наличие CI в организации, функциональные характеристики;
- документации для релиза до его осуществления.

Только авторизованные и корректные CI должны использоваться для поддержки услуг. Если в рамках проверок выявлены нарушения, они должны быть немедленно устранены, а результаты проверок отображены в соответствующих отчетах.

Как и любой другой процесс, SACM имеет свои ключевые показатели производительности. Применяются следующие метрики:

- процентное улучшение в управлении расписаниями в рамках жизненного цикла активов;
- ускоренная идентификация активов, вызвавших сбои в работе услуг;
- уменьшение влияния инцидентов и ошибок на CI;
- процент лицензий, которые используются, к общему количеству купленных (в идеале 100%);
- увеличение качества информации о CI в CSM;
- уменьшение использования нелицензионного ПО;

Информацию, формируемую в рамках SACM, используют все процессы в рамках жизненного цикла услуг.

Управление Релизами и Установкой (Release & Deployment Management RDM)

Процесс Управления Релизами и Установкой является частью этапа «Внедрения» и отвечает за тестирование возможностей для предоставления услуг.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса управления ИТ активами и конфигурациями.
- формирование и согласование планов релизов и развертывания с заказчиками и инвесторами;
- гарантия того, что каждый пакет для релиза состоит из набора связанных и совместимых компонентов;
- осуществление управления релизом и его компонентами в рамках процессов Внедрения;

- гарантия того, что все пакеты для релизов могут быть протестированы, отслежены, проверены, установлены или устранены (при необходимости);
- гарантия того, что все изменения управляются в рамках деятельности по управлению релизами и развертыванием;

Деятельность по процессу:

- Планирование
- Подготовка, тестирование и внедрение релиза или сборки
- Сборка и тестирование

Входами процесса Управления релизами и развертыванием являются:

- авторизованные Запросы на изменения;
- Проектная документация (SDP);
- пакет уровней услуг (SLP);
- План обеспечения непрерывности бизнеса и ИТ;
- приобретенные активы и компоненты с их документацией;
- модели и планы сборки;
- требования и спецификации сред для сборки, тестирования, пилотирования, развертывания, обучения и восстановления;
- политика и проект релизов от этапа Проектирования;
- модели релизов и развертывания;
- критерии входа и выхода для каждой стадии развертывания и релиза.

Выходами процесса Управления релизами и развертыванием являются:

- План релиза и развертывания;
- завершенные Запросы на изменения для деятельности в рамках релиза и развертывания;
- оповещение об услуге;
- обновленный Каталог услуг с информацией о новой или измененной услуге;
- новые протестированные возможности услуги и среды;
- новая или измененная документация сервис-менеджмента;
- пакет услуг, учитывающий требования бизнеса
- Пакет уровней услуг (SLP);
- SLA, OLA и другие контракты;
- протестированные планы непрерывности;
- полный и актуальный перечень конфигурационных единиц;
- план мощностей, соответствующий планам бизнеса;
- подготовленный пакет релизов
- отчет о внедрении.

Участники процесса:

- Комитет по Управлению Изменениями
- Менеджер по Релизам и сборкам
- Менеджер по внедрению

Ключевые показатели производительности Управления релизами и развертыванием можно разделить на два класса:

Заказчики и бизнес:

- уменьшение отклонения значений производительности услуг от требуемых заказчиками и бизнесом;
- уменьшение количества инцидентов, связанных с услугами;
- увеличение удовлетворенности пользователей и заказчиков предоставленными услугами;
- уменьшение неудовлетворенности пользователей и заказчиков.

Поставщики услуг:

- уменьшение необходимых ресурсов и затрат для диагностирования и исправления инцидентов и проблем в рамках развертывания и производства;

- увеличение использования стандартизированного подхода к Внедрению, в том числе процессов, документации и стандартов;
- уменьшение несовпадений между информацией, предоставляемой проверками конфигураций, и реальной ситуацией.

Ключевые моменты процесса:

- Комитет по Управлению Изменениями является владельцем процесса
- ИТ департамент управляет процессом в рамках ИТ сервисов

Единица релиза (Release Unit) – компоненты услуги, которые обычно компонуются вместе и выпускаются в рамках одного релиза. Единица релиза обычно включает в себя компоненты, необходимые для выполнения какой-либо полезной функции. Например, Единицей релиза может быть настольный компьютер, включающий в себя программное, аппаратное обеспечение, лицензии, документацию и т. п.

Важно определить подходящий уровень Единицы релиза для каждого актива и компонента. Необходимо учитывать следующие факторы:

- простота и количество изменений, необходимых для релиза и развертывания;
- количество ресурсов и времени, необходимое для сборки, тестирования и развертывания;
- сложность взаимосвязей между единицей и остальными услугами и компонентами;
- хранение, доступное в рамках сборки, тестирования, распространения и эксплуатации.

Для развертывания релиза необходимо разработать различные планы, в частности, Планы релизов и развертывания. Они должны определять:

- охват и контекст релиза;
- оценку рисков для релиза;
- организации и отдельные лица, которых затронет релиз;
- инвесторов, которые утвердили запрос на изменение;
- команду, ответственную за релиз;
- стратегию предоставления и развертывания;
- ресурсы для релиза и развертывания;
- количество изменений, которые могут быть осуществлены.

В рамках Внедрения должны быть определены критерии, которые позволят установить успешность выполнения каждой стадии релиза и развертывания. Результат выполнения либо принимается (pass), либо отклоняется (fail).

Перед передачей услуги в промышленную эксплуатацию, необходимо совершить ряд действий по сборке и тестированию различных сред. Среды, необходимые для релиза:

- среда сборки* – используется для сбора и комплектования пакета релиза;
- единичная среда тестирования* – используется для проверки функциональности, производительности, восстанавливаемости и полезности отдельных компонентов услуги;
- комплект сред тестирования* – используется для проверки функциональности, производительности, восстанавливаемости и полезности комплекта компонентов услуги;
- среда интеграции* – используется для сборки и интеграции компонентов услуги;
- среда тестирования услуги* – используется для тестирования всех аспектов объединенной архитектуры услуги;
- среда тестирования релиза* – используется для установки, сборки и тестирования пакета релиза в контролируемой среде; обычно совмещена со средой тестирования услуги.
- среда тестирования готовности к эксплуатации* – для тестирования возможностей услуги и ее компонентов перед передачей в промышленную эксплуатацию;
- среда, симулирующая бизнес-среду;*
- среда, симулирующая Управление услугами;*
- среда для обучения;*
- среда для пилотирования;*
- среда для резервного копирования и восстановления.*

Для тестирования услуги на маленькой части пользователей используются пилоты.

Пилот (Pilot) – ограниченное развертывание услуги, релиза или процесса в среде промышленной эксплуатации. Пилот используется для сокращения рисков и получения обратной связи, а также приемки от пользователей. Для пилотирования также должны формироваться планы.

Планирование сборки пакета релизов содержит следующие процедуры:

- проверка критериев входа/выхода;
- взаимодействие с инвесторами:
- управление контрактами и их деталями;
- доведение до инвесторов информации о предлагаемых изменениях, выгоде, которую они могут принести и сопутствующих затратах, и рисках
- обучение персонала и передача знаний;
- установление услуг и активов в виде имеющихся контрактов;
- согласование графиков;
- разработка механизмов и инструментов для:
- сборки, тиражирования, продвижения, распространения, контроля, инсталляции и активации релизов;
- управления лицензиями и авторскими правами.
- настройка систем и обучение пользователей для работы с новой или измененной услугой;
- разработка возможностей и ресурсов для сервис-менеджмента;
- оценка готовности целевой группы к использованию релиза;
- определение и согласование критериев для выхода.

В рамках составления планов развертывания необходимо ответить на следующие вопросы:

- для кого предназначено развертывание?
- кто будет пользователями?
- есть ли какие-то особенности месторасположения?
- где пользователи?
- кто еще должен быть подготовлен к релизу?
- когда необходимо завершить развертывание?
- почему необходимо развертывание?
- какие факторы успеха и критерии выхода?
- каковы текущие возможности поставщика услуг?

Далее разрабатываются *Планы снабжения* и предоставления. Они определяют следующее:

- как и когда релиз и его компоненты будут предоставляться?
- какие имеются команды сопровождения, и что будет в случае задержки?
- как отследить прогресс в предоставлении и необходимость его завершения?
- есть ли возможность защищенного хранения, если потребуется?

Прежде чем добавлять какие-то действия в планы развертывания, необходимо осуществить *финансовое планирование*. Оно рассматривает вопросы выделения средств для обеспечения деятельности, покупки необходимого оборудования и лицензий, имеющиеся контракты и обязательства.

После того, как детальные планы для каждой деятельности в рамках Управления релизами и развертыванием составлены, наступает *этап подготовки к сборке, тестированию и развертыванию*. На этом этапе происходит оценка рисков, возможных проблем и несоответствий в проектной документации. Оценка проверяет, принесет ли изменение желаемые результаты. Формируется отчет, в котором содержатся рекомендации об утверждении изменения или его отклонении.

Если изменение утверждено, наступает *этап сборки и тестирования*. Ключевые аспекты, которыми необходимо управлять в рамках этого этапа:

- использование сред сборки и тестирования;
- стандартизация и интеграция;
- управление конфигурациями;

- контроль версий, управление базовым состоянием, контроль входов и выходов этапа сборки и тестирования;
- ведение отчетности, которая позволит осуществить сборку снова при возникновении необходимости;
- управление наглядностью тестирования
- контроль доступа к физическим компонентам и технологиям;
- проверка выполнения требований безопасности;
- проверка деятельности – все необходимые условия выполнены;
- управление вопросами среды – кондиционирование, электропитание, физическое место, пожарная сигнализация и т. п.
- проверка готовности релиза к передаче на следующую стадию;
- передача релиза на следующую стадию.

В ITIL вводится понятие «базовое состояние».

Базовое состояние (Baseline) – зафиксированное состояние, используемое как ориентир (контрольная точка). Трактовка зависит от контекста. В контексте Внедрения базовое состояние может быть использовано для возврата инфраструктуры к исходной конфигурации в случае, если внедрение релиза оказалось неудачным. Информация о базовых состояниях конфигураций хранится в CMS.

Для сборки релиза необходимо объединить множество компонентов, активов и продуктов от внешних и внутренних поставщиков. Деятельность по приобретению компонентов включает в себя:

- взаимодействие с процессами снабжения для приобретения компонентов;
- сбор;
- проверка, мониторинг и ведение отчетности о качестве поступающих конфигурационных единиц и компонентов услуг;
- обеспечение того, что наличие лицензии можно будет доказать при возникновении необходимости;
- ответные действия в случае, если качество, полученное на практике, отличается от ожидаемого, и оценка влияния снижения качества на внедрение в целом;
- обновление статусов конфигурационных единиц в SACM.

После того, как все необходимое куплено, документация готова, можно приступить к сборке пакета релизов. При сборке релизов важно понимать, что продукт поступит скоро в промышленное производство, следовательно, использованные в рамках сборки процедуры должны быть повторимы в случае необходимости.

Ключевые *этапы деятельности сборки пакета релизов*:

- комплектование и интеграция компонентов релиза;
- создание документации для сборки и релиза
- инсталляция и проверка пакета релиза;
- отправка уведомлений всем заинтересованным участникам о том, что пакет релиза готов для инсталляции и использования.

Если тестирование пакета релизов прошло успешно, релиз и его составляющие попадают под контроль Управления конфигурациями. С этого момента все изменения в пакете релизов осуществляются через Управление изменениями.

В рамках *тестирования операционной готовности* проводятся следующие тесты:

- тестирование готовности к развертыванию – проверяет то, что процессы, процедуры и системы развертывания могут развертывать, устанавливать, назначать и списывать пакет релизов и соответствующую ему услугу в среде производства/развертывания;
- тестирование Управление услугами – проверка того, что производительность услуги может быть измерена и проконтролирована в процессе промышленной эксплуатации;
- тестирование группы эксплуатации – проверяет, что сервисные подразделения смогут управлять услугой в процессе промышленной эксплуатации;

- тестирование уровня услуг – проверка соответствия новой или измененной услуги требованиям уровня услуг;
- тестирование пользователей – проверка того, что пользователи имеют доступ к новой или измененной услуге и могут ее использовать;
- тестирование интерфейса поставщика услуг – проверка того, что интерфейсы, поддерживающие услугу, функционируют;
- тестирование развертывания – проверка того, что услуга корректно развернута для каждой целевой группы или среды.

После проведения указанных выше тестов наступает *заключительный этап тестирования – «репетиция услуги»*. Это метод тестирования, в котором создаются условия, максимально приближенные к условиям реальной эксплуатации. Он должен выявить ошибки и неработающие процессы, прежде чем они повлияют на бизнес в процессе промышленной эксплуатации. Проводится перед непосредственным развертыванием услуги. Как вариант может осуществляться в виде пилота – то есть на маленькой группе реальных пользователей услуги.

После успешного тестирования или пилотирования можно приступить к развертыванию услуги. На начальном этапе составляются детальные планы развертывания, и производится оценка рисков. Планы должны быть утверждены, а Запросы на изменения авторизованы процессом Управления изменениями. Только после этого услуга готова к развертыванию.

В рамках развертывания могут выполняться следующие действия:

- перенос финансовых активов;
- Перенос/переход бизнеса и организации
- окончательное оформление организационной структуры, ролей и ответственностей;
- установление связей между изменениями организации, ролей и ответственностей;
- убедиться в том, что люди могут приспособиться к новым практикам;
- убедиться в том, что люди понимают планы и процедуры обеспечения непрерывности.

Развертывание услуги – развертывание релиза, в том числе действия по распространению и установке услуги, поддерживающих услуг, приложений, инфраструктуры и функциональных возможностей. В этот этап входят следующие деятельности:

- распространение и развертывание услуги и ее компонентов в заданных границах времени;
- сборка, установка и настройка услуги и ее компонентов на работу с новой или преобразованной информацией;
- тестирование системы и услуг в рамках инсталляции, формирование отчетов об инсталляции и тестировании;
- фиксация всех проблем, сбоев, ошибок, инцидентов и расхождений с планами;
- корректирование всех расхождений, которые не выходят за рамки проектных ограничений.

Отзыв услуги – действия, предпринятые для того, чтобы релиз можно было отозвать в случае возникновения необходимости.

Поддержка в начале эксплуатации (Early Life Support или ELP) – поддержка, предоставляемая в отношении новой или измененной услуги в течение некоторого времени непосредственно после того, как услуга была введена в эксплуатацию. Во время поддержки в начале эксплуатации поставщик услуг может пересматривать ключевые показатели производительности, уровни услуги и наблюдаемые пороговые значения, а также задействовать дополнительные ресурсы для Управления инцидентами и Управления проблемами.

Обзор и завершение развертывания. Обзор развертывания включает в себя следующие действия:

- организация опросов и исследований удовлетворенности пользователей, инвесторов и заказчиков новой или измененной услугой;
- выявить недостигнутые критерии качества;
- проверить завершенность всех необходимых действий, исправлений и изменений;
- пересмотреть незавершенные изменения и убедиться в том, что для них выделены финансовые средства и назначены ответственные исполнители;
- пересмотреть целевые показатели производительности и успешности;

- убедиться, что все проблемы, связанные с ресурсами, возможностями, мощностями и производительностью, решены до завершения развертывания;

- проверить то, что все проблемы, известные ошибки и обходные решения согласованы с инвесторами, заказчиками и пользователями. Обходное решение (Workaround) – уменьшение или устранение влияния инцидента или проблемы, для которых в текущий момент недоступно полное разрешение.

- пересмотреть все риски и выявить те, которые влияют на эксплуатацию и поддержку услуги;
- проверить то, что избыточные активы извлечены из обращения;
- проверить готовность услуги к передаче от ELP в промышленную эксплуатацию.

Процесс управления релизами и установкой также используется в процессе сопровождения сервиса. Он в основном используется в пределах ИТ департамента.

При внедрении процесса управления релизами и установкой необходимо определить следующие важные атрибуты:

Определить тип релиза или установки:

- Плановый (Planned)
- Внеплановый (Unplanned)

Определить категория релиза или установки:

- Проект (Project)
- Обновление (Patch)
- Важное обновление (Major patch)
- Небольшие обновления (Minor patch)
- Сборка (Build)

Определить, по возможности категоризацию воздействия с указанием метрик:

- Высокое (High) воздействие
- Среднее (Medium) воздействие
- Низкое (Low) воздействие

Определить, по возможности уровень риска, при применении релиза или установки:

- Высокий (High) риск воздействие
- Среднее (Medium) риск воздействие
- Низкое (Low) риск воздействие
- Воздействие не определённо (Not assessed)

Определение источников, приводящих к появлению релиза:

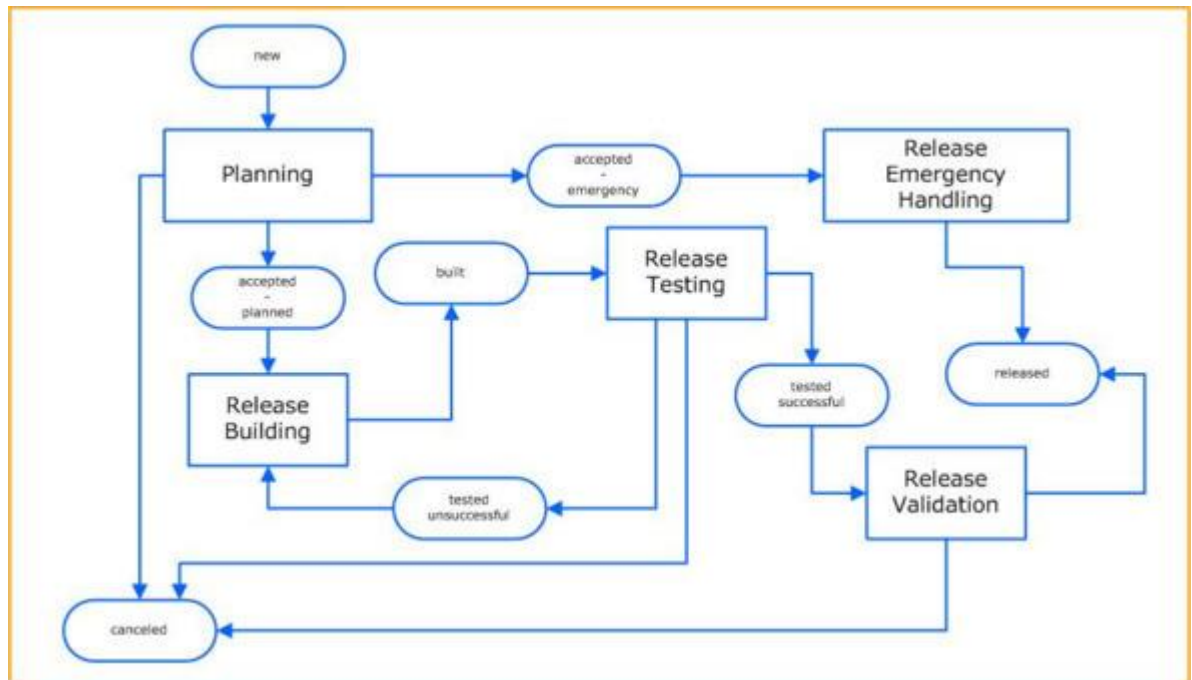
- Запросы на изменения со стороны бизнеса
- Запросы на изменения со стороны Безопасности
- Анализ инцидентов (Процесс управления инцидентами)
- Анализ запросов (Процесс управления запросами)
- Анализ проблем (Процесс управления проблемами)
- Мониторинг событий и логов
- Анализ релизов (Процесс управления Релизами)
- Запросы на Улучшение Сервиса

Статусы изменений:

- Инициирован (Initiate)
- Одобрённый (Approved)
- Активный (In progress)
- В ожидании (On pending)
- Приостановленный (On hold)
- Проверенный (Validated and Reviewed)
- Выполненный (Completed)
- Закрытый (Closed)

- Активность проигнорирована (skipped)

Определение групп выполнения и подтверждения изменений при запуске релиза. Зависит от организационной структуры ИТ департамента, классификации изменений и т.п.



Результаты запуска релиза соответствуют статусу изменений:

- Удачно выполненный (Successfully implemented)
- Выполненный с незначительными проблемами (Implemented with Issues)
- Частично выполненный (Partially implemented)
- Не выполненный (Failed)
- Отказанный (Rejected)
- Отозванный (Cancelled)
- Не одобренный (Unauthorized)

Оценка и Тестирование (Service Validation & Test SVT)

Процесс Управления Оценкой и Тестированием сервисов является составной частью Контроля и управления качеством. Данный процесс отвечает на такие вопросы как:

- Формирование процесса Управления Оценкой и Тестированием сервисов.
- планирование и последующая реализация процессов тестирования и подтверждения, которые представят объективные доказательства того, что услуги предоставляют заявленную ценность заказчикам, пользователям и инвесторам;
- оценка качества релиза и его компонентов;
- идентификация, оценка и улаживание проблем, ошибок и рисков в процессе Внедрения.

Действия по процессу:

Формирование процесса

Оценка функциональных возможностей сервиса

Подготовка тестовой среды

Проведение тестов

Оценка результатов тестирования

Оценка планируемых и фактических показателей

Оценка соответствия

Входами процесса Подтверждения и тестирования услуг являются:

пакет услуг;

Пакет уровня услуг (SLP);

интерфейсы поставщика услуг;

проектная документация (SDP);

планы релизов и развертывания;

критерии приемки;

Запросы на изменения.

Процесс управления Изменениями

Процесс управления Портфелем ИТ Сервисов

Процесс управления каталогом ИТ Сервисов

Процесс управления Требованиями

Процесс управления Доступностью

Процесс управления Мощностями

Процесс управления Информационной Безопасности

ИТ архитектура

Основными выходами процесса Подтверждения и тестирования услуг являются:

- формирование базового состояния конфигураций для проведения тестирования;

- осуществляемые тесты;

- результаты этих тестов;

- анализ результатов – сравнение реальных и прогнозируемых данных, анализ выявленных в ходе тестирования рисков.

Подтверждение (Validation) – деятельность, которая гарантирует, что новая или измененная услуга, процесс, план или другой результат отвечает нуждам бизнеса. Подтверждение гарантирует, что требования бизнеса удовлетворены, даже если они могли измениться по отношению к исходному результату проектирования.

Подтверждение и тестирование услуг (Service Validation and Testing) – процесс, ответственный за подтверждение и тестирование новой или измененной услуги. Подтверждение и тестирование услуг удостоверяет, что услуга соответствует ее спецификации проектирования и будет отвечать потребностям бизнеса.

Прежде чем начинать тестирование, необходимо сформировать стратегию тестирования. Стратегия тестирования определяет подход к организации тестирования и обработке его результатов. Она может применяться ко всей организации, набору услуг или отдельной услуге. Каждая стратегия должна согласовываться с инвесторами, так как они выделяют деньги на ее реализацию.

Содержание стратегии тестирования:

Цели и задачи тестирования;

контекст;

стандарты, требования законов и регуляторов;

контракты и соглашения;

охват и организация:

- команды поставщика услуг;

- организация тестирования;

- третьи стороны, стратегические партнеры, поставщики;

- бизнес-единицы и их месторасположение;

- пользователи и заказчики.

процесс тестирования:

- управление и контроль тестированием – запись, мониторинг прогресса, ведение отчетности;

- планирование и оценка тестирования;

- действия в рамках тестирования – планирование, реализация и документирование тестов и их результатов.

*метрики тестирования и улучшения
идентификация объектов тестирования:*

- пакет услуг;
 - пакет уровня услуг;
 - модель услуг, отображающая структуру и динамику развития услуг;
- план эксплуатации услуг;*

планы сервис-менеджмента:

- критические элементы, на которых необходимо сконцентрировать тестирование;
- месторасположение бизнес-единиц, на которых будет осуществляться тестирование.

интерфейсы поставщика услуг;

подход:

- выбранная модель тестирования;
- уровни тестирования;
- подходы к тестированию;
- степень независимости реализации, оценки и анализа тестирования;
- повторное использование – опыт, практика, знания и результаты тестирований в прошлом;
- распределение по времени;
- разработка и повторное использование проектов, инструментов, сценариев и данных для тестирования;
- контроль изменений и исправление ошибок;
- система измерения.

критерии:

- приема/отклонения;
- входа и выхода для каждой стадии тестирования;
- остановки или повторного запуска тестирования.

требования к людям:

- роли и ответственности;
- составление расписания тренингов для персонала;
- требования к степени вовлеченности заинтересованных лиц – поставщиков услуг, поставщиков, заказчиков, пользователей.

требования к среде:

- среды тестирования, которые будут использованы, их расположение, организация и техническое оснащение;
- требования к каждой среде тестирования;
- планирование и ввод в эксплуатацию сред тестирования.

результаты:

- обязательная и опциональная документация;
- планы тестирования;
- спецификации тестирования – процедуры, проект, обоснование тестирования;
- результаты тестирования и отчеты;
- проверка отчетов;
- суммарные отчеты по тестированию.

Существует множество подходов к тестированию. Они могут комбинироваться или использоваться по отдельности в зависимости от того, что конкретно тестируется:

- обзор документации;
- моделирование и измерение
- подход, основанный на рисках
- подход, основанный на соответствии стандартам;
- подход, основанный на опыте
- симуляция;
- тестирование по сценариям;
- разыгрывание ролей;
- макетирование;
- тестирование в лабораторных условиях;

- регрессивное тестирование;
- пилотирование в отдельном помещении;
- пилотирование в среде промышленной эксплуатации.

Чтобы оптимизировать использование ресурсов в рамках тестирования, необходимо расставить приоритеты тестирования в зависимости от значимости услуги для бизнеса, влияния услуги и рисков, ассоциированных с ней.

Тестирование гарантии. Как уже говорилось, пользователи видят и измеряют ценность услуги в двух составляющих – гарантии и полезности. При этом для каждой услуги определяются четкие показатели гарантии.

В рамках тестирования гарантии могут проводиться:

- тестирование доступности;
- тестирование мощности;
- тестирование непрерывности;
- тестирование безопасности.

Тестирование простоты использования услуги используется, как правило, для организации работы потенциальных пользователей;

Тестирование соответствия контрактам и требованиям регуляторов. Тестирование проверяет, что все критерии контрактов и требования регуляторов выполнены и удовлетворены;

Тестирование Управления услугами – тестирование процессов в рамках Управления услугами;

Операционное тестирование – включает в себя множество тестов, зависящих от типа услуги. Типичные тесты включают:

- нагрузочные тесты и стресс-тесты – проверяют способность услуги работать на требуемом уровне на доступных мощностях. В качестве мощностей может рассматриваться полоса пропускания сети, ресурсы сервис-деска, доступные лицензии, мощность процессора, доступная память и т. п.;
- тестирование безопасности – все услуги должны быть рассмотрены со стороны их влияния на аспекты безопасности организации;
- тестирование восстанавливаемости – тестирование плана восстановления, который должен быть разработан для каждой услуги.
- регрессивное тестирование – такое тестирование повторяет успешные тесты и сравнивает вновь полученные значения с предыдущими. Оно позволяет протестировать услуги и их компоненты, которые раньше работали без сбоев и ошибок.

Не все деятельности в рамках тестирования выполняются последовательно, многие могут выполняться параллельно. *Управление тестированием* включает в себя следующие действия:

- планирование ресурсов для тестирования;
- распределение что и когда должно тестироваться;
- управление инцидентами, ошибками, проблемами, рисками;
- проверка того, что известные ошибки и документация обработаны;
- отслеживание прогресса и сбор данных от обратной связи с различными этапами тестирования;
- осуществление незначительных изменений для уменьшения ошибок в промышленной эксплуатации;
- фиксация базового состояния конфигураций;
- тестирование набора метрик, анализ, ведение отчетности и управление.

Метрики тестирования используются для оценки деятельности в рамках тестирования. Они позволяют персоналу, ответственному за тестирование, контролировать прогресс и успешность тестирования.

Планирование и проектирование тестирования. Планирование и проектирование тестирования рассматривает следующие вопросы:

- обеспечение ресурсами;

- определение дат контрольных точек;
- согласованное время предоставления результатов тестирования;
- точка и время приемки;
- финансовые требования.

Ключевые показатели производительности процесса Подтверждения и тестирования услуг:

- первостепенные показатели отражают ценность для бизнеса и заказчиков;
- раннее подтверждение того, что услуга сможет предоставлять предсказанную ценность;
- уменьшение негативного влияния ошибок и инцидентов в промышленной эксплуатации;
- более эффективное использование ресурсов;
- уменьшение задержек в тестировании, которые влияют негативно на бизнес;
- улучшение понимания новой или измененной услуги;
- четкое понимание ролей и ответственностей, относящихся к новой или измененной услуге;
- затраты и ресурсы, необходимые от пользователей и заказчиков.

второстепенные показатели – внутренние по отношению к поставщику услуг. Эти показатели отражают эффективность и результативность тестирования:

- объем работ и стоимость настройки среды тестирования;
- объем работ для нахождения дефектов;
- уменьшение повторяющихся ошибок
- уменьшение количества ошибок/дефектов на поздних стадиях тестирования и в процессе производства;
- повторное использование данных тестирований;
- количество ошибок на каждой стадии жизненного цикла;
- количество и процентное соотношение ошибок, которые были обнаружены в ходе тестирования;
- инциденты, найденные в ходе тестирования, как процент от общего количества инцидентов, произошедших в ходе эксплуатации;
- количество известных ошибок, задокументированных на ранних стадиях тестирования.

Оценка Изменений (Change Evaluation CHE)

Оценка (Evaluation) – процесс, ответственный за проведение оценки новой или изменяемой услуги для обеспечения управления рисками и помощи в принятии решения о продолжении проведения изменения. Фактическая производительность услуги оценивается через сравнение с ожидаемой производительностью. Процесс также находит причины расхождения этих значений и управляет ими. Оценка фактической производительности любого изменения в услугах является важной частью сервис-менеджмента. Поставщик услуг может оценить, насколько реалистичны были его прогнозы в отношении услуг, и выявить причины несоответствия фактических значений ожиданиям.

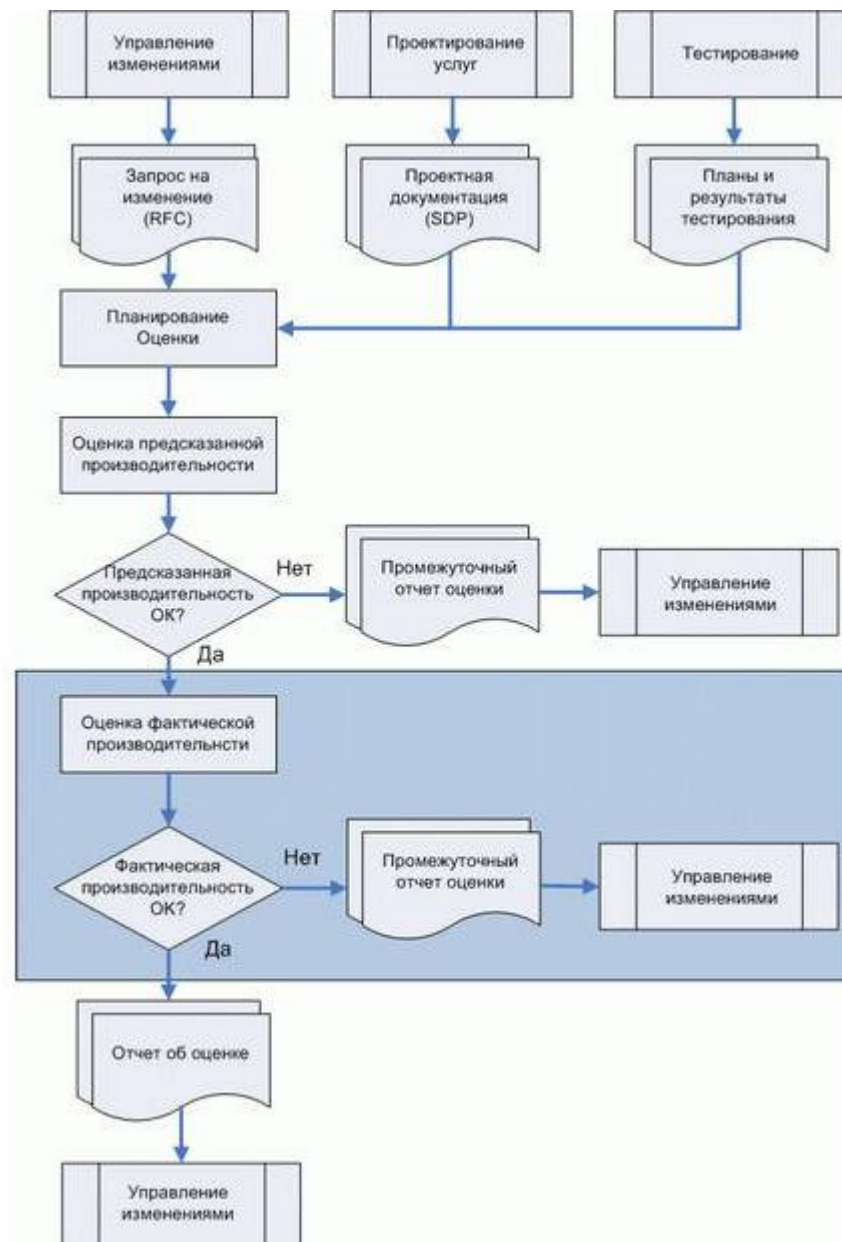
Данный процесс отвечает на такие вопросы как:

- Формирование процесса Управления оценкой Изменений.

Оценка должна рассматривать как запланированные, так и незапланированные эффекты изменения. При этом для простоты считается, что запланированные эффекты всегда приносят выгоду. Незапланированные эффекты гораздо труднее предсказать, и обычно они проявляются уже в процессе эксплуатации. Незапланированные эффекты, в отличие от запланированных, не всегда приносят пользу.

Деятельность по процессу:

- Утверждение процесса Управления оценкой Изменений
- Оценка результатов процесса изменений
- Формирование процесса
- Оценка процесса Управления Изменениями
- Оценка процесса Управления Релизами и Установками



Входы процесса:

Процесс Управления Изменениями
 Процесс Управления Оценкой и Тестирования сервисов
 Процесс управления Изменениями
 Процесс управления Портфелем ИТ Сервисов
 Процесс управления каталогом ИТ Сервисов
 Процесс управления Требованиями
 Процесс управления Доступностью
 Процесс управления Мощностями
 Процесс управления Внедрениями и поддержкой
 Процесс управления Релизами и Установками
 Процесс Управления Оценкой и Тестированием сервисов
 Процесс управления Информационной Безопасности
 ИТ архитектура
 Пакет услуг,
 Проектная документация,
 Критерии приемки услуг,

Результаты тестов.

Выходы процесса:

Подписанный протокол решения ИТ комитета

Отчет об оценке Управления Изменениями

Ключевые показатели производительности для процесса Оценки:

со стороны заказчиков/бизнеса:

- уменьшение отличий между фактической производительностью и той, которая нужна заказчикам;

- уменьшение количества инцидентов, связанных с услугой.

внутренние показатели:

- количество «провалившихся» проектов (должно стремиться к нулю);

- уменьшение времени на проведение оценки.

Запланированные эффекты описываются в документации к изменению вместе с метриками, которые позволят измерить эффективность изменения.

Приведем основные аспекты для оценки эффективности изменения:

Способность поставщика услуг – способность поставщика услуг или сервисной единицы осуществлять свою деятельность в соответствии с требованиями;

Переносимость – способность или мощность услуги принять изменение или релиз;

Организационное регулирование – способность организации принять предлагаемое изменение. Например, обновлены ли все имеющиеся услуги для того, чтобы гладко провести процесс внедрения новой услуги? Или: у группы внедрения есть все необходимые доступы?

Ресурсы – квалифицированный персонал, финансовые средства, инфраструктура, приложения и другие ресурсы, необходимые для внедрения услуги;

Моделирование и измерение – мера совпадения предсказанного поведения услуги (в процессе моделирования) с фактическим;

Люди – люди в рамках системы и влияние изменения на них;

Использование – подходит ли услуга для использования? Будет ли она доступной, надежной, безопасной и т. п.?

Цель – подходит ли услуга для осуществления поставленной перед ней цели? Сможет ли она предоставить требуемую производительность? Поможет ли она удалить ограничения?

Результатом проведения Оценки становится отчет, состоящий из следующих секций:

- перечень рисков – риски, которые остались после применения контрмер и действий по их уменьшению;

- отчет по расхождениям – разница между предсказанной и фактической производительностью;

- заключение об утверждении и проверки на соответствие техническим требованиям (если требуется);

- рекомендации процессу Управления изменениями о том, стоит принять или отклонить изменение.

Управление Базой Знаний (Knowledge Management KNM)

Управление знаниями (Knowledge Management) – процесс, отвечающий за сбор, анализ, сохранение и предоставление знаний и информации в Организации. Первичная цель Управления знаниями – увеличение эффективности путем снижения необходимости в повторном поиске

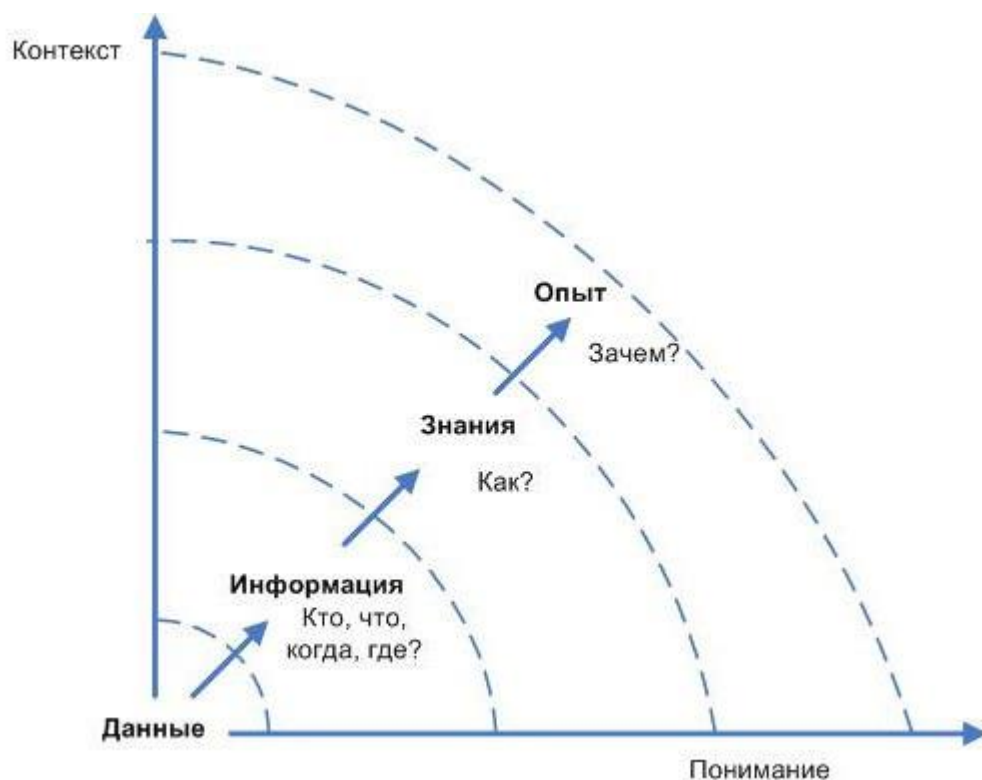
знаний. Процесс отвечает за то, чтобы нужная информация поступала к компетентному лицу своевременно для поддержки в принятии решений.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса Управления Базой Знаний.
- Порядок взаимодействия с отделом Кадров

Задачи процесса:

- повышение результативности поставщика услуг, качества услуг и удовлетворенности заказчиков, а также снижение затрат;
- обеспечение понимания персоналом ценности предоставляемых заказчикам услуг;
- обеспечение своевременного доступа персонала к следующей информации:



Данные-Информация-Знания-Мудрость (Data-to-Information-to-Knowledge-to-Wisdom или DIKW)

Действия по процессу:

- Разработка стратегии управления знаниями
- Утверждение процесса Управления Базой Знаний
- Организация процесса передачи знаний
- Организация процесса обучения сотрудников
- Организация процесса тестирования и аттестации
- Формирование процесса Управления Базой Знаний
- Создание Базы Знаний

Входы процесса:

- Этап внедрения сервисов

Этап сопровождения сервисов
Процесс управления проблемами

Выходы процесса:
Система Управления Знаниями
Знания

Важно, чтобы люди и организации, участвующие в процессе, четко понимали метрики его успешности и эффективности. Для оценки эффективности Управления знаниями можно использовать множество критериев.

В общем случае критериями процесса Управления знаниями могут быть:

- успешное внедрение и эксплуатация услуг с небольшим количеством ошибок;
- улучшение ответов на запросы бизнеса;
- улучшение доступности стандартов и политик и управления ими;
- распространение знаний;
- уменьшение времени и «сил», необходимых для поддержки и управления услугами;
- уменьшение времени на поиск информации, необходимой для диагностирования и решения проблем и ошибок;
- уменьшение зависимости знаний от персонала.

Критерии для бизнеса и заказчиков:

- уменьшение пользовательских ошибок в результате эффективной передачи знаний;
- уменьшение времени на решение проблем в результате того, что персонал лучше обучен и может воспользоваться SKMS;
- улучшения для пользователей:
- быстрое разрешение запросов;
- способность решения проблем без помощи извне;
- проблемы и вопросы решаются на том уровне, на котором появились, и не передаются выше.
- уменьшение времени внедрения и поддержки на ранних стадиях эксплуатации услуги.

Критерии для поставщика услуг:

- использование знаний, измеренное в:
- количество запросов к SKMS;
- среднее время на поиск необходимой информации.
- ошибки, выявленные в ходе проверок или о которых сообщил персонал;
- участие персонала в форумах для предоставления поддержки посредством сбора и обмена знаниями;
- степень повторного использования процедур, проектов тестирования, сценариев и т. п., описанных в документации;
- удовлетворенность персонала организацией обмена знаниями.

Данные-Информация-Знания-Мудрость (Data-to-Information-to-Knowledge-to-Wisdom или DIKW) – способ представления взаимосвязей между данными, информацией, знанием и мудростью. Концепция DIKW показывает, каким образом каждое из перечисленных понятий базируется на остальных.

Рассмотрим термины в составе DIKW:

Данные — набор дискретных фактов о событиях. В рамках Управления знаниями над ними выполняются следующие действия:

- сбор точных данных;
- анализ и преобразование в информацию;
- определение наиболее значимых данных.

Информация — структурированные данные. Информация, как правило, хранится в слабоструктурированных формах — документах, e-mail, файлах. Управление знаниями предназначено для того, чтобы информацию можно было легко запросить, найти и использовать. Это необходимо для исключения ошибок, облегчения поиска и предотвращения избыточных работ.

Знания — комплект накопленных взглядов, опыта, идей, ценностей и суждений. Люди получают знания, опираясь на свой собственный опыт и на опыт других людей, а также путем анализа информации, поступающей из различных источников. Знания предоставляют и структурируют информацию таким образом, чтобы ее можно было легко использовать для принятия решений.

Мудрость — предоставляет ультимативный процесс понимания материального и способность принимать решения, основываясь на логических рассуждениях.

Знания процессов Управления услугами хранятся в Системе управления знаниями и услугами.

Система управления знаниями и услугами (Service Knowledge Management System SKMS) — набор инструментов и баз данных, которые используются для управления знаниями и информацией. SKMS включает Систему управления конфигурациями, также как и другой инструментарий и базы данных. SKMS сохраняет, управляет, обновляет, и представляет всю информацию, которая необходима поставщику услуг для управления полным жизненным циклом ИТ-услуг. SKMS представляет собой большую базу знаний, которая содержит в частности:

- опыт персонала;
- записи об окружающей обстановке.
- возможности, требования и ожидания
- уровень квалифицированности персонала.

Рассмотрим основные действия и принципы в рамках Управления знаниями.

Формирование стратегии. Для организации Управления знаниями, как и для всех предыдущих процессов, необходимо разработать стратегию. Стратегия должна рассматривать следующие вопросы:

- модель управления;
- планируемые и уже проводимые организационные изменения и соответствующие им изменения ролей и ответственностей;
- определение ролей и ответственностей
- политики, процедуры, методы и процессы
- технологические и другие требования;
- метрики измерения производительности процесса.

Особенно внимание в стратегии должно быть уделено сбору значимых для организации знаний, данных и информации. В частности:

- помощь организации в определении знаний, которые будут полезны;

•проектирование структурированного процесса для организации, отбора, хранения и предоставления информации. Это позволит людям улучшить понимание значимых для организации областей;

- сбор информации от разных процессов;
- формирование новых знаний;
- получение необходимой информации из сторонних источников;
- сбор знаний из внешних источников (например, Интернета, партнеров, публикаций и т. п.) и их адаптация под нужды организации.

Передача знаний. Для Управления знаниями крайне важно наладить обмен информацией в рамках организации. На практике часто именно в этом заключается основная сложность. Традиционными средствами передачи знаний в рамках организации являются тренинги и документация.

Управление данными и информацией. Для эффективного управления данными и информацией Управлению знаниями важно ответить на следующие вопросы:

- какие знания нужны для принятия решений?
- какие условия необходимо контролировать?
- какие данные доступны?
- сколько стоит сбор и управление информацией?

После нахождения ответов на представленные вопросы необходимо определить требования к собираемой информации. Очень часто организации накапливают большое количество данных и информации без понимания того, как они будут использованы в дальнейшем.

Когда требования определены, можно построить «*архитектуру информации*». Под этим подразумевается выполнение следующих действий:

- формирование и регулярное обновление модели управления информацией, которая позволит гибко, экономно и своевременно создавать, использовать информацию и управлять ею;
- определение системы, которые позволят оптимизировать использование информации путем эффективного управления данными и информацией;
- формирование системы классификации информации в рамках организации.

На следующем шаге определяются процедуры управления данными и информацией. Они должны включать в себя механизмы, позволяющие:

- определить данные и информацию;
- определить процедуры управления данными и информацией и сделать их доступными для тех, кому они нужны;
- хранить и восстанавливать;
- устанавливать роли и ответственности для отдельных единиц информации;
- определять и публиковать права, обязанности и условия, необходимые для осуществления доступа к информации и данным;
- делать резервные копии информации и данных;
- определить требования для пересмотра хранимых информации и данных, например, внедрение новых технологий;
- собирать и хранить запросы к информации.

В рамках Управления данными и информацией необходимо также разработать планы по улучшению процедур и процесса в целом.

Использование SKMS для поддержки принятия решений в рамках организации.

ЭТАП СОПРОВОЖДЕНИЯ (Operation Stage)

Введение

Основной целью Эксплуатации услуг является координирование процессов и деятельности, необходимых для предоставления услуг заказчикам на согласованных уровнях. Эксплуатация также ответственна за непрерывное управление технологиями, поддерживающими услуги.

Цели и задачи:

- Формирование процесса эксплуатации сервиса и его поддержка.
- Организация ежедневных действия и операций по сопровождению сервиса
- Организация процесса мониторинга и отчетности по производительности ИТ сервисов
- Предоставление и сопровождение ИТ сервисов

Данный этап определяется следующими процессами:

- Управление событиями (Event Management)
- Управление инцидентами (Incident Management)
- Управление запросами (Request Fulfilment)
- Управление проблемами (Problem Management)
- Управление доступом (Access Management)

Данный этап регламентируются следующими функциями:

- Техническое управление (Technical Management)
- Управление приложениями (Application Management)
- Операционное управление (Operation Management)
- Контроль ИТ операций (IT Operations Control)
- Системы Обеспечения (Facility Management)

Управление Событиями (Event Management EVM)

Управление событиями (Event Management) – процесс, ответственный за управление событиями в течение жизненного цикла. Управление событиями одна из главных деятельности операционного управления ИТ.

Данный процесс отвечает на такие вопросы как:

- Формирование процесса управления Событиями.

Деятельность по процессу:

Утверждение процесса управления Событиями
Формирование процесса управления Событиями
Классификация Событий
Определение реакции на события
Определение инструментов по мониторингу событий
Информирование по событиям
Определение события
Фильтрация событий
Определение значимости события
Корреляция событий
Формирование триггеров на события
Реакция на события
Обзор действий
Закрытие событий
Документирование

Входы процесса:

Процесс Управления Изменениями
Политика Информационной Безопасности

Процесс управления Изменениями Политика Информационной Безопасности

Выходы процесса:

Процесс Управления Изменениями

Процесс управления инцидентами

Политика Информационной Безопасности

Процесс управления Изменениями

Политика Информационной Безопасности

Для того чтобы быть эффективным, операционное управление должно знать состояние инфраструктуры и ее компонентов, а также отслеживать любые отклонения от нормальной работы. Управление событиями реализуется с помощью систем мониторинга и контроля, которые основаны на двух типах инструментов:

инструменты активного мониторинга – опрашивают ключевые конфигурационные единицы с целью выяснения их статуса и доступности. Любое отклонение вызовет предупреждение, который перенаправляется необходимой команде или инструменту для принятия необходимых действий.

Активный мониторинг (Active Monitoring) – мониторинг конфигурационных единиц или услуг, использующий автоматизированные регулярные проверки для отслеживания текущего статуса объекта мониторинга.

инструменты пассивного мониторинга – обнаруживают и собирают события, без принятия каких-либо ответных действий.

Пассивный мониторинг (Passive Monitoring) – мониторинг конфигурационной единицы, услуги или процесса, который основывается на предупреждениях или уведомлениях о текущем состоянии объекта мониторинга.

Необходимо сразу отметить разницу между мониторингом и Управлением событиями. Эти процессы очень похожи, но, тем не менее, имеют отличия. Управление событиями сфокусировано на обнаружении значимых событий, касающихся статусов услуг и инфраструктуры. Мониторинг же следит за всеми событиями, и, по сути, имеет более широкий охват. Например, мониторинг может отслеживать состояние устройства, чтобы удостовериться, что оно функционирует в установленных рамках, даже если устройство не генерирует никаких событий. Таким образом, Управление событиями является частью системы мониторинга.

Фактически, Управление событиями может контролировать любой аспект сервис-менеджмента. Объектами Управления событиями могут быть:

конфигурационные единицы;

условия среды (пожар или обнаружение дыма);

мониторинг использования лицензий на программное обеспечение;

безопасность;

нормальная активность (например, использование приложений или производительность сервера).

Ценность Управления событиями для бизнеса косвенная. Тем не менее, можно выделить следующие преимущества, которые дает Управление событиями бизнесу:

Предоставляет механизмы для раннего обнаружения инцидентов. Во многих случаях Управление событиями позволяет обнаружить инцидент и принять соответствующие действия до того, как он значительно повлияет на услугу в целом.

При интеграции с другими процессами сервис-менеджмента может повысить их эффективность. Он может сообщить об изменениях или отклонениях статусов, что позволит соответствующей команде своевременно предпринять необходимые действия.

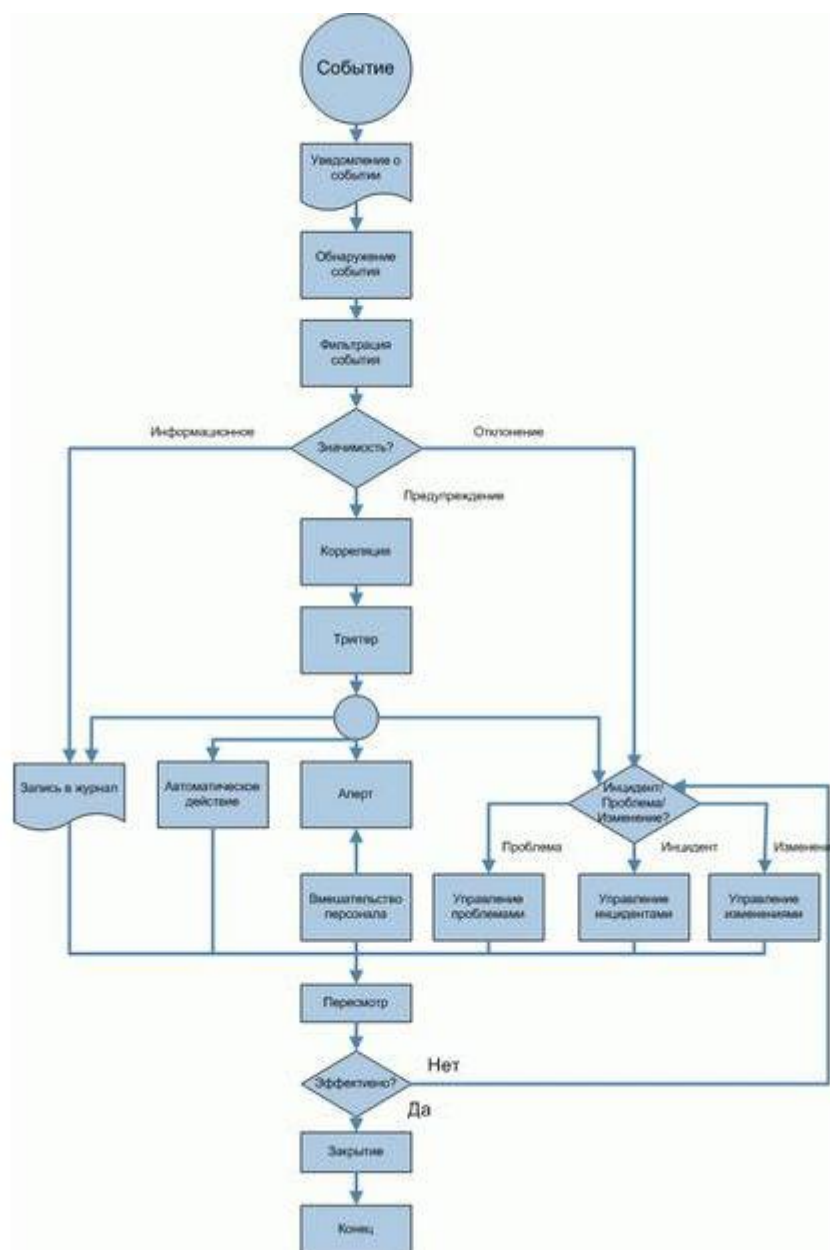
Раннее оповещение о необходимости обновления процедур или ресурсов;

Управление событиями основано на автоматизированных операциях, что увеличивает эффективность и позволяет задействовать персонал на более «креативные» работы, в частности, проектирование новых услуг и поиск путей по улучшению существующих.

Управление событиями работает со следующими типами событий:

- события, сигнализирующие о регулярной операции – , например, уведомления о том, что работы в соответствии с графиком выполнены;
- аутентификация пользователя для использования приложения;
- E-mail достиг получателя;
- события, отмеченные как отклонения, например, попытка входа в приложение с использованием некорректного пароля;
- нестандартная ситуация в работе бизнес-процесса, которая может потребовать дальнейших действий;
- использование CPU выше установленной нормы;
- установка неизвестных приложений.

события, отмеченные как нестандартные, но при этом не являющиеся отклонениями. При обнаружении подобных событий необходим более детальный мониторинг.



Разного рода события возникают постоянно, но при этом не все события нужно регистрировать и обнаруживать. Важно, чтобы люди, участвующие в проектировании,

разработке, развертывании и поддержке услуг, четко понимали, какие именно события необходимо отслеживать.

Конфигурационные единицы в большинстве случаев выдают предупреждения в случае выполнения определенных условий. Возможность формировать эти предупреждения должна быть спроектирована и встроена в конфигурационные единицы. Многие конфигурационные единицы генерируют предупреждения с использованием открытого стандарта SNMP.

В идеальном случае на этапе Проектирования формируется стандартный набор событий, которые необходимо отслеживать в отношении конкретных конфигурационных единиц. В рамках этапа Внедрения этот набор тестируется и настраивается.

После того, как предупреждение сформировано, специальный агент в системе обнаруживает его, «читает» и анализирует значимость события. Следующий шаг – фильтрация событий. На этом этапе выносится решение о том, будет ли данное событие проигнорировано или его необходимо передать менеджменту для осуществления необходимых ответных действий. Если событие игнорируется, оно просто записывается в журнал событий (лог). Никаких других действий не выполняется. Фильтрация является первым шагом к классификации событий. Этап фильтрации, по сути, является необязательным.

Каждая организация имеет свои критерии для оценки значимости события, но рекомендуется использовать как минимум три категории событий:

- Информационное событие
- Предупреждение
- Ошибка

Информационное событие – относится к событию, которое не требует никаких действий и не является отклонением. Такие события просто записываются в логи и используются для слежения за работой системы и ее компонентов, или контроля выполнения каких-то операций. Они также могут использоваться для сбора статистики и дальнейших исследований. Примерами информационных событий могут быть вход пользователя в систему или успешное завершение транзакции.

Предупреждение – этот тип события формируется тогда, когда услуга или устройство приближается к пороговым значениям. Предупреждения предназначены для того, чтобы соответствующий сотрудник, процесс или инструмент проверили ситуацию более детально и приняли необходимые меры для предотвращения отклонения. Примерами предупреждений могут быть использование памяти сервера более 75% или увеличение количества коллизий в сети.

Ошибка – этот тип событий сигнализирует о том, что услуга или устройство функционируют неправильно (за пределами нормы). Это значит, что нарушаются SLA и OLA, что, как следствие, приводит к негативному влиянию на бизнес в целом. Примерами отклонений могут послужить выход из строя сервера, сегмент сети не отвечает на запросы и т.п.

Если событие отмечено как значительное, необходимо определить точно его значимость и необходимые ответные действия – это этап корреляции. Корреляция обычно выполняется частью средства управления под названием «Correlation Engine», которая применяет к событию набор правил и критериев в определенном порядке. Основная идея в том, что событие может повлиять на бизнес, а правила помогут определить степень и тип этого влияния. В механизме корреляции событий прописывается способ реагирования на событие, например, что делаем при первом, втором и последующих проявлениях данного предупреждающего события, при сочетании или последовательности ряда событий – отклонений, одиночном, но имеющем очень серьезные для заказчика последствия, отклонении.

Примеры того, что может использовать Correlation Engine для оценки:

количество похожих событий (например, большое количество попыток неправильного ввода пароля может свидетельствовать о попытке взлома устройства);

количество конфигурационных единиц, генерирующих похожие события;
сопровождает ли событие какие-либо специфичные действия с данными или кодом;
является ли событие отклонением;
категория события;
назначение приоритета событию и т. п.

Механизм, который инициирует ответные действия, называется триггером. Существует множество типов триггеров, каждый из которых спроектирован для инициализации конкретных действий. Например,

Триггеры инцидентов, которые формируют запись в Системе управления инцидентами и, соответственно, запускают процесс Управления инцидентами;

Триггеры изменений, которые формируют RFC и инициируют процесс Управления изменениями;

Скрипты, которые выполняют определенные действия, например, перезагрузку устройства;

Триггеры баз данных, которые ограничивают доступ пользователей к определенным областям базы или удаляют/создают записи в ней.

Следующий этап – выбор ответных действий. Существует множество вариантов ответных действий, которые при этом могут комбинироваться.

Ниже приведены примеры вариантов ответных действий:

Запись события в лог. Вне зависимости от того, какое ответное действие будет выбрано, хорошей практикой является формирование записи о событии в логе. Должна быть стандартная процедура для операционного персонала, предусматривающая периодический анализ логов, а также четкие инструкции о том, как использовать конкретный лог. Также необходимо помнить о том, что информация в логах может не иметь значения до возникновения инцидента. В рамках Управления событиями нужно определить период хранения логов перед тем, как они будут заархивированы или удалены.

Автоматические ответные действия. Для регулярных и «понятных» событий можно разработать автоматические ответные действия. Триггер запустит их и затем проверит результат выполнения. Если что-то пошло не так, будет сформирована запись о проблеме или инциденте. Примерами автоматических ответных действий могут быть:

- перезагрузка устройства;
- повторный запуск услуги;
- изменение параметра устройства;
- блокировка приложения для предотвращения несанкционированного доступа и т. п.

Предупреждение и вмешательство людей. Предупреждение служит для уведомления о событии людей, которые имеют необходимые навыки и знания для его разрешения. При этом события должны содержать как можно более полную информацию о событии, на основании которой человек сможет принять правильное решение.

Создание Запроса на изменение (RFC). В Управлении событиями есть две точки, где могут быть созданы RFC:

при возникновении отклонения. Например, проверка компьютера показала, что на нем установлено три неавторизованных приложения. В этом случае необходимо сформировать RFC, который поможет процессу Управления изменениями устранить отклонение.

на этапе корреляции была определена необходимость изменения. В данном случае на этапе корреляции определяется, что наиболее подходящим ответным действием будет изменение чего-то.

Создание записи об инциденте. Если Correlation Engine определяет то, что определенный набор событий является инцидентом, создается запись об инциденте. Запись об инциденте должна быть максимально полной и отражать связи со всеми событиями, относящимися к инциденту.

Создание записи о Проблеме или формирование связи с уже имеющейся записью. Инциденты обычно связаны с определенными записями о проблемах. При возникновении инцидента важно связать его с соответствующей записью о проблеме, а если такой нет – создать ее.

Особые типы инцидентов. В некоторых случаях событие может являться отклонением, но при этом не влиять непосредственно на услуги. Такие инциденты не включаются в расчет времени простоя и относятся скорее с проблем операционного характера. Информация о них должна быть записана в соответствующий лог и передана персоналу, который разбирается с инцидентами этого типа.

Каждый день может происходить десятки и сотни событий и зачастую невозможно детально рассматривать каждое событие. Обзорные действия предназначены для проверки того, как были отработаны инциденты, не пропущены ли какие-то события, сбора статистических данных и т. п. При этом обзорные действия не должны повторять то, что было сделано до этого.

Основными сложностями и рисками для Управления событиями являются недостаточное финансирование, выбор оптимального уровня фильтрации событий и упущение момента для своевременного развертывания агентов в рамках инфраструктуры.

Для того чтобы Управление событиями было эффективным, его механизмы должны быть разработаны на этапе Проектирования услуг в рамках процессов Управления доступностью и Управления мощностями. Но при этом Управление событиями не является статичным – в ходе эксплуатации услуг могут появляться новые требования и события, которые необходимо отслеживать. Проектирование Управления событиями должно включать следующее:

Инструментарий – что может быть отслежено в отношении конфигурационных единиц и как можно воздействовать на них. Другими словами, это точное определение и проектирование того, как контролировать и мониторить инфраструктуру и услуги. В рамках определения инструментария необходимо ответить на следующие вопросы:

что необходимо мониторить?

какой тип мониторинга необходим?

когда необходимо формировать событие?

какая информация должна содержаться в событии?

для кого предназначены сообщения о событиях?

Сообщения об ошибках должны отображать критичные ошибки, свидетельствующие о сбое или вероятности его возникновения.

Механизмы обнаружения событий и формирования предупреждений. Проектирование этих механизмов требует:

знания взаимосвязей всех бизнес-процессов, которые контролируются с помощью Управления событиями;

знания SLA для каждой услуги, поддерживаемой конфигурационной единицей;

знания того, кто поддерживает конфигурационную единицу;

знания того, какие значения параметров конфигурационной единицы являются нормальными, а какие нет;

понимание того, что именно нужно знать для эффективного управления конфигурационной единицей;

знания информации, которая может помочь эффективной поддержке конфигурационной единицы;

осознания важности совокупности одинаковых или похожих событий;

понимание взаимосвязей конфигурационных единиц;

доступности информации об известных ошибках, полученной от поставщика или из предыдущего опыта.

Определение пороговых значений для каждой конфигурационной единицы. При этом значения могут изменяться в зависимости от многих обстоятельств. Например, максимальное количество пользователей, получающих доступ к серверу, зависит от того, какие именно работы они на нем выполняют.

Показатели процесса и метрики, которые можно использовать для измерения эффективности Управления событиями:

- количество событий по категориям;
- количество событий по значимости;
- количество событий, которые потребовали участия персонала;
- количество инцидентов, вызванных известными ошибками и проблемами;
- количество одинаковых инцидентов (или повторяющихся);
- количество инцидентов, связанных с проблемами производительности;
- количество инцидентов, свидетельствующих о наличии потенциальных проблем с доступностью и т. п.

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Количество событий

Количество событий по сервисам

Количество зарегистрированных событий

События, связанные с инцидентами

События, связанные с проблемами

Управление Инцидентами (Incident Management INM)

Процесс Управления Инцидентами является частью этапа «Сопровождения».

Управление инцидентами (Incident Management) – процесс, отвечающий за управление жизненным циклом всех инцидентов. Основная цель Управления инцидентами – скорейшее восстановление услуги для пользователей.

Данный процесс отвечает на такие вопросы как:

Формирование процесса управления Инцидентами.

Деятельность по процессу:

Утверждение процесса управления Инцидентами

Формирование процесса управления Инцидентами

Классификация Инцидентов

Определение реакции на Инциденты

Идентификация инцидента

Регистрация инцидента

Классификация и категоризация инцидента

Определение приоритетов

Первичная диагностика

Эскалация инцидента

Расследование и диагностика

Разрешение инцидента

Обзор значимых инцидентов

Реактивация инцидента
Закрытие инцидента
Документирование
Контроль процесса
Отчетность по процессу

Входы процесса:

Процесс Управления Изменениями
Процесс Управления Событиями
Политика Информационной Безопасности
Регистрация заявки
CMDB
Коммуникация с сотрудниками

Выходы процесса:

Утверждение политик и процедур
Регистрация проблем
Регистрация запросов
Регистрация запросов на изменения
Регистрация запросов на доступ
Формирование знаний

Участники процесса:

ИТ комитет, бизнес руководители
Сотрудники ИТ департамента
Представители Департамента Безопасности
Менеджер процесса

Ключевые моменты процесса:

ИТ департамент является владельцем процесса

Процесс Управления Инцидентами вводит такие понятия как:

Степень Воздействия (Impact / Severity) – определяет границы воздействия инцидента.

Срочность (Urgency) – определяет время решения инцидента.

Приоритет (Priority) – комбинация степени воздействия и срочности инцидента. При эскалации инцидента приоритет сохраняется. В зависимости от Соглашения об Уровне Сервиса (SLA) определяет сроки и порядок реагирования на инцидент.

Эскалация (Escalation) – перенос инцидента на другой уровень. Различают:

Функциональная / горизонтальная – привлечение большего количества сотрудников данного уровня

Иерархическая / вертикальная – переход на верхний уровень поддержка

Запросы на обслуживание

Основные рекомендации для сотрудника подразделения Поддержки Пользователя при работе с пользователем:

Надо дать возможность пользователю объяснить проблему и высказать свою точку зрения

В процессе общения с клиентом концентрируйте внимание на том, чем вы можете помочь клиенту.

Попросите пользователя продемонстрировать проблему.

В конце разговора резюмируйте коротко все то, что было сказано пользователем, чтобы быть уверенным что поняли правильно.

Не спрашивайте вопросы так, чтобы он повторял только что сказанное. Это может создать у него впечатление, что его не слушают.

Не обвиняйте и не критикуйте клиента.

Старайтесь не использовать выражения «... я не знаю... вы должны...»

При организации процесса управления инцидентами необходимо ввести следующие важные элементы процесса:

Полная матрица категоризации приоритета инцидента, если имеется необходимое программное обеспечение:

Или упрощенная категоризация определения инцидента:

Инциденты Первой категории – Важные и Срочные

Инциденты Второй категории – Важные и Не Срочные

Инциденты Третьей категории – Не Важные и Срочные

Инциденты Четвертой категории – Не Важные и Не Срочные

Определить, по возможности категоризацию воздействия с указанием метрик:

Высокое (High) воздействие – Инцидент воздействует на всех пользователей, или Инцидент приводит к деградации сервиса более чем на 50% или полному отказу, или Инцидент затрагивает критические компоненты сервиса

Среднее (Medium) воздействие – Инцидент воздействует на (значительную или нет) группу пользователей, или Инцидент приводит к ощутимой деградации сервиса в пределах 20—50%, но в пределах SLA, или Инцидент затрагивает критические, но зарезервированные компоненты сервиса

Низкое (Low) воздействие – Инцидент воздействует на одного пользователей, или Инцидент приводит к незначительной, не более чем на 20%, деградации сервиса, или Инцидент затрагивает не критические или второстепенные компоненты сервиса

Определить категоризацию срочности с указанием метрик:

Высокая (High) срочность – Инцидент требует немедленного вмешательства

Средняя (Medium) срочность – Инцидент требует вмешательства, но время разрешения в пределах SLA

Низкая (Low) срочность – Инцидент не требует немедленного вмешательства

1 - Highest Priority 9 – Lowest Priority		URGENCY		
		High	Medium	Low
IMPACT	High	1	2	3
	Medium	4	5	6
	Low	7	8	9

Порядок реагирования для каждой категории инцидентов:

Время реакции на инцидент – максимальное время, в течении которого ИТ департамент обязуется среагировать на инцидент. Как правило это идентификация, классификация, назначение инцидента на группу поддержки с информированием сотрудника, контакт с пользователем и т.п.

Время разрешения инцидента – максимальное время, в течении которого ИТ департамент обязуется разрешить инцидент.

Время закрытия инцидента – максимальное время ожидания реакции сотрудника, после которого инцидент будет закрыт.

Определение источников поступления инцидентов:

- Контакт с пользователем
- Телефонный звонок
- Электронная почта
- Электронный портал
- Системы мониторинга

Статусы инцидента:

- Активный
- В ожидании
- Разрешенный
- Отказанный
- Закрытый

Классификация инцидентов по типам и подтипам (зависит от специфики организации, предпочтениям и т.п.):

- Проблемы с сервисом X
- Проблемы с аппаратным обеспечением
- Проблемы с операционным обеспечением
- Проблемы с приложением
- Проблемы с конфигурацией
- Проблемы с доступом
- Проблемы с производительностью
- Прочие проблемы
- Проблемы конечных пользователей
- Проблемы с аппаратным обеспечением
- Проблемы с операционным обеспечением
- Проблемы с приложением
- Проблемы с конфигурацией
- Проблемы с доступом
- Проблемы с производительностью
- Прочие проблемы
- Прочие проблемы

Определение групп разрешения инцидентов. Зависит от организационной структуры ИТ-департамента, классификации инцидентов и т.п.:

- Оператор центра Поддержки Пользователей
- Первая линия поддержки
- Вторая линия поддержки
- Третья линия поддержки и поддержка производителя

Определение категорий разрешения инцидента:

Самостоятельное разрешение
Отказан
Разрешен
Закрыт

Определение метрик и показателей оценки эффективности и результативности процесса.

Кроме элементов, выше указанных, необходимо также определить следующие элементы:
порядок информирования пользователя, сотрудника ИТ и менеджера проекта или супервайзера на различных этапах жизни инцидента.

Метрики соглашений

Порядок эскалации инцидента

Памятка оператору, для быстрой идентификации и классификации инцидента

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Количество инцидентов

Соотношение открытых инцидентов

Тенденция инцидентов (рост, снижение)

Количество инцидентов на устройство

Количество инцидентов на пользователя

Количество инцидентов, выполненных в срок

Среднее время реакции

Среднее время разрешения инцидента

Процент инцидентов, выполненных удаленно

Количество ошибочных инцидентов

Среднее время устранения инцидента

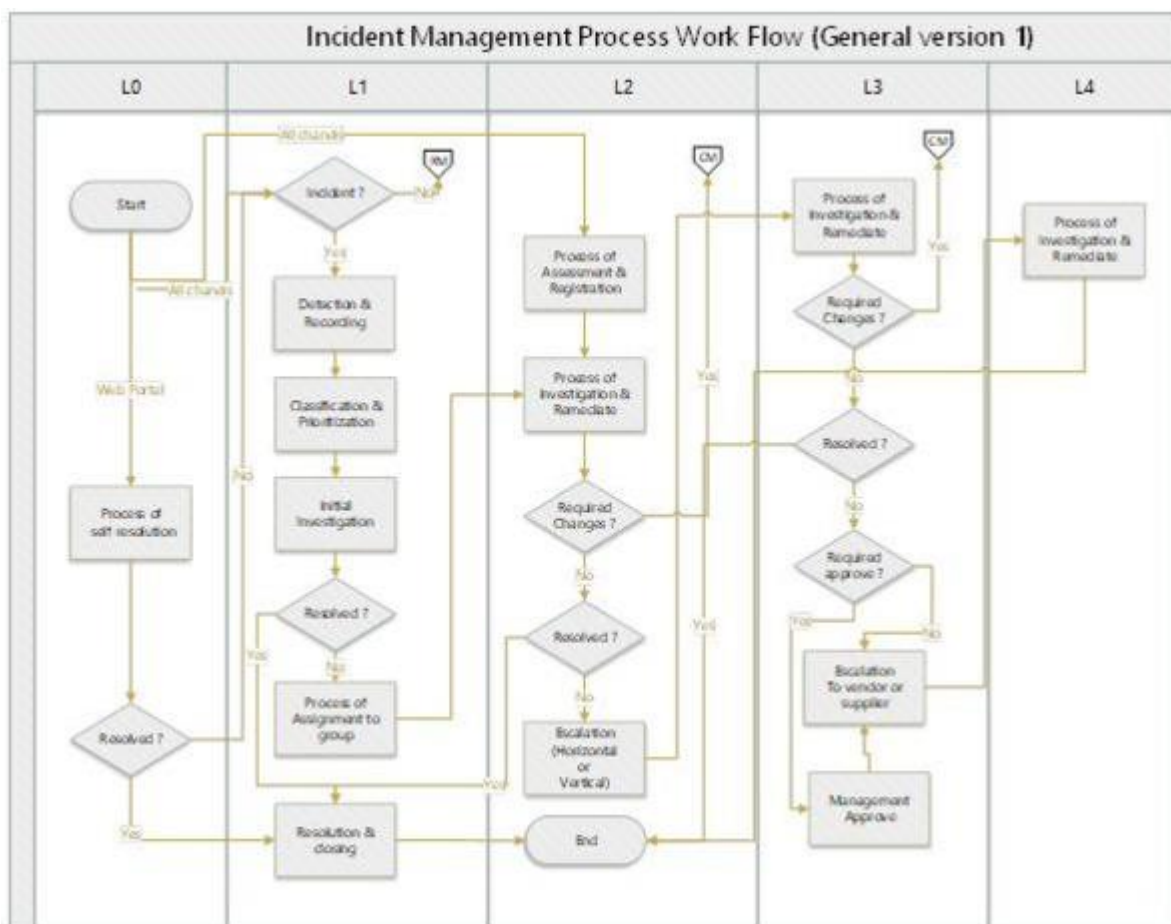
Количество повторных инцидентов

Количество инцидентов решенных с помощью изменений

Количество «важных» инцидентов

Количество «срочных» инцидентов

Количество инцидентов по операторам



Карта процесса Управления Инцидентами

Управление Запросами (Request Management RQM)

Процесс Управления Запросами является частью этапа «Сопровождения». Данный процесс отвечает на такие вопросы как:

Формирование процесса управления Запросами.

Процесс является наиболее сложным с точки зрения внедрения, так как выходит за рамки департамента, и требует вовлечения других подразделений организации.

Деятельность по процессу:

Утверждение процесса управления Запросами

Интеграция процесса управления запросами в Систему Управления ИТ сервисами в организации

Формирование процесса управления Запросами

Классификация Запросов по типам

Формирование шаблонов запросов по типам

Формирование списка заранее одобренных типовых запросов

Определение групп выполнения запросов

Определение групп одобрения запросов по типам

Формирование под-процессов по типам запросов

Определение реакции на Запросы

Определение метрик и показателей процесса

Интеграция процесса управления запросами с прочими процессами

Определение под-процесса классификации и категоризации запросов

Разрешение конфликтов

Входы процесса:

Процесс Управления Изменениями
Процесс Управления Событиями
Процесс управления Инцидентами
Политика Информационной Безопасности
Процесс управления Изменениями
Процесс управления Событиями
Процесс управления Инцидентами
Политика Информационной Безопасности
Организационная структура организации
Порядок одобрения запросов

Выходы процесса:

Предоставление процесса самообслуживания
Запросы на изменения
Запросы на доступ
Регистрация инцидентов
Регистрация проблем

Участники процесса:

ИТ комитет
Сотрудники ИТ департамента
Представители Департамента Безопасности
Представители бизнеса организации

Ключевые моменты процесса:

ИТ департамент является владельцем процесса

При внедрении процесса управления запросами необходимо определить следующие важные атрибуты:

Определить, по возможности категоризацию воздействия и срочности с указанием метрик:

Высокое (High) воздействие – Запрос воздействует на всех пользователей или критичен для бизнеса, или Запрос затрагивает критические компоненты сервиса

Среднее (Medium) воздействие – Запрос воздействует на (значительную или нет) группу пользователей или бизнеса, или Запрос затрагивает критические, но зарезервированные компоненты сервиса

Низкое (Low) воздействие – Запрос воздействует на одного пользователей или не критичен для бизнеса, или Запрос затрагивает не критические или второстепенные компоненты сервиса.

Высокая (High) срочность – Запрос требует немедленного вмешательства или выполнения

Средняя (Medium) срочность – Запрос требует вмешательства, но время разрешения в пределах SLA

Низкая (Low) срочность – Запрос не требует немедленного вмешательства

Порядок реагирования для каждой категории запросов:

Время реакции на запрос – максимальное время, в течении которого ИТ департамент обязуется среагировать на инцидент. Как правило это идентификация, классификация, назначение инцидента на группу поддержки с информированием сотрудника, контакт с пользователем и т.п.

Время разрешения запроса – максимальное время, в течении которого ИТ департамент обязуется разрешить инцидент.

Время закрытия запроса – максимальное время ожидания реакции сотрудника, после которого инцидент будет закрыт.

Определение источников поступления запросов:

Контакт с пользователем

Телефонный звонок
Электронная почта
Электронный портал
Системы мониторинга

Статусы запроса:
Инициирован (Initiate)
Одобрённый (Approved)
Активный (In progress)
В ожидании (On pending)
Приостановленный (On hold)
Проверенный (Validated and Reviewed)
Выполненный (Completed)
Закрытый (Closed)
Активность проигнорирована (skipped)

Классификация запросов по типам и подтипам (зависит от специфики организации, предпочтениям и т.п.):

Запрос на предоставление сервиса (новый сервис, новое оборудование и т.п.)
Запрос на обслуживание (предоставление доступа к имеющимся сервисам)
Запрос на предоставление информации
Запрос на предоставление доступа

Определение групп выполнения и подтверждения запросов. Зависит от организационной структуры ИТ департамента, классификации запросов и т.п.:

Оператор центра Поддержки Пользователей
Группы подтверждения запросов (по процессам)
Первая линия поддержки
Вторая линия поддержки
Третья линия поддержки и поддержка производителя

Результаты выполнения запроса:
Удачно выполненный (Successfully implemented)
Выполненный с незначительными проблемами (Implemented with Issues)
Частично выполненный (Partially implemented)
Не выполненный (Failed)
Отказанный (Rejected)
Отозванный (Cancelled)
Не одобренный (Unauthorized)

Определение типовых под-процессов для различных запросов
Определение метрик и показателей оценки эффективности и результативности процесса

Кроме элементов, выше указанных, необходимо также определить следующие элементы: порядок информирования пользователя, сотрудника ИТ и менеджера проекта или супервайзера на различных этапах жизни запроса.

Метрики соглашений
Порядок эскалации запроса
Памятка оператору, для быстрой идентификации и классификации запроса

Критерии результативности – (KGI)
Критерии эффективности – (KPI)
Количество запросов
Количество выполненных запросов
Количество не правильных запросов

Карта процесса

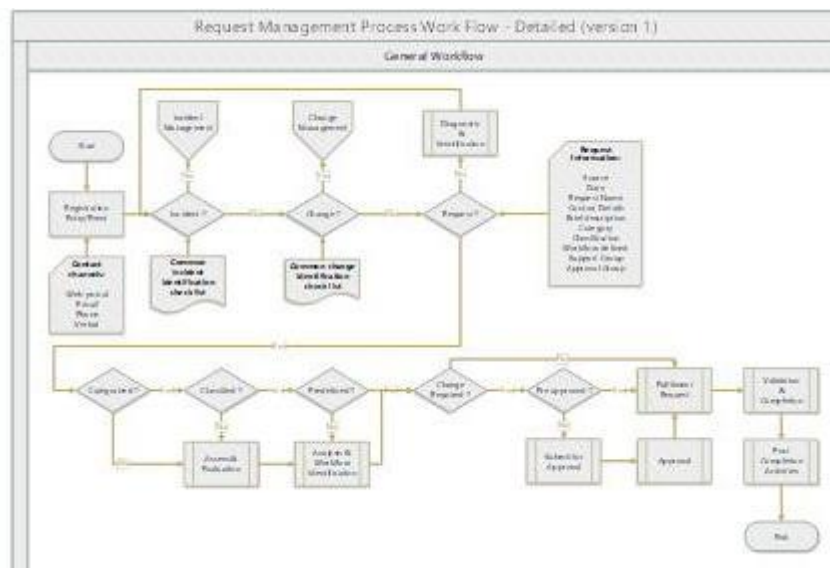
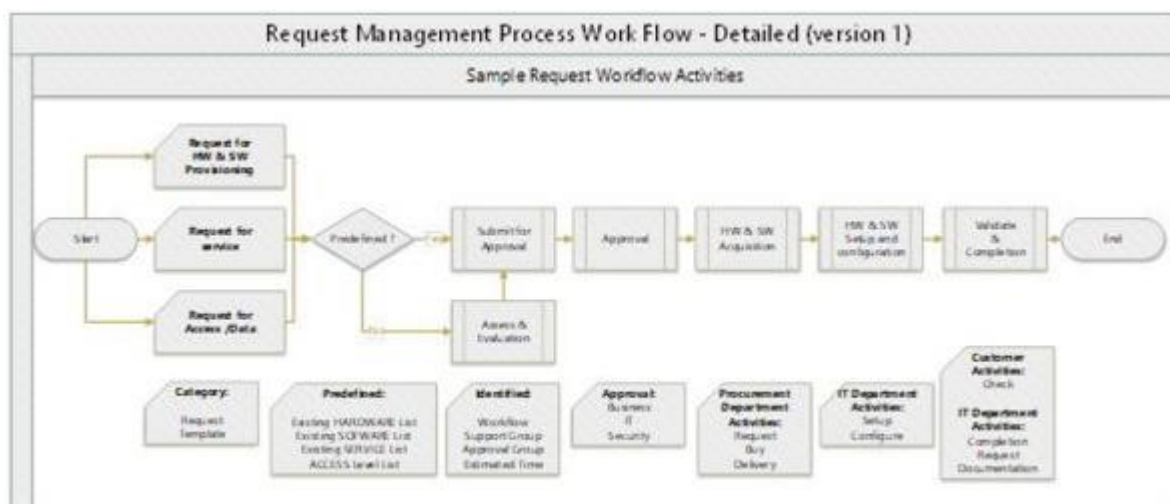


Диаграмма: Процесс Управления Запросами



Процесс Управления Запросами – активность рабочего процесса

Управление Проблемами (Problem Management PRM)

Процесс Управления Проблемами является частью этапа «Сопровождения».

Данный процесс отвечает на такие вопросы как:

Формирование процесса управления Проблемами.

Действия по процессу:

Утверждение процесса управления Проблемами

Формирование процесса управления Проблемами

Классификация Проблемам

Определение реакции на Проблемы

Реактивное управление проблемами

Про активное управление проблемами

Идентификация проблем

Регистрация проблем

Классификация и категоризация проблем

Определение приоритета проблем
Исследование и диагностика
Разрешение проблемы
Заккрытие проблемы
Обзор значимых проблем

Входы процесса:

Процесс Управления Изменениями
Процесс Управления Событиями
Процесс управления Инцидентами
Процесс управления Запросами
Политика Информационной Безопасности

Выходы процесса:

Регистрация проблем
Нахождение обходных решений
Формирование знаний
Запросы на изменения

Участники процесса:

ИТ комитет
Сотрудники ИТ департамента
Представители Департамента Безопасности

Ключевые моменты процесса:

ИТ департамент является владельцем процесса

Рекомендуемые восемь шагов по решению проблемы:

Установка симптомов
Определение сферы влияния проблемы
Установить, что было изменено
Выбрать наиболее вероятные причины
Применить решение
Протестировать решение
Оценить потенциальный эффект решения
Задokumentировать решение

При внедрении процесса управления проблемами необходимо определить следующие важные атрибуты:

Определить, по возможности категоризацию воздействия и срочности с указанием метрик:

Высокое (High) воздействие – Проблема воздействует на всех пользователей или критична для бизнеса, или Проблема затрагивает критические компоненты сервиса.

Среднее (Medium) воздействие – Проблема воздействует на (значительную или нет) группу пользователей или бизнеса, или Проблема затрагивает критические, но зарезервированные компоненты сервиса.

Низкое (Low) воздействие – Проблема воздействует на одного пользователей или не критичен для бизнеса, или Проблема затрагивает не критические или второстепенные компоненты сервиса.

Высокая (High) срочность – Проблема требует немедленного вмешательства или выполнения.

Средняя (Medium) срочность – Проблема требует вмешательства, но время разрешения в пределах SLA

Низкая (Low) срочность – Проблема не требует немедленного вмешательства.

Порядок реагирования для каждой категории проблем:

Время разрешения проблемы – максимальное время, в течении которого ИТ департамент обязуется разрешить проблему.

Определение источников поступления проблем:

Анализ инцидентов (Процесс управления инцидентами)

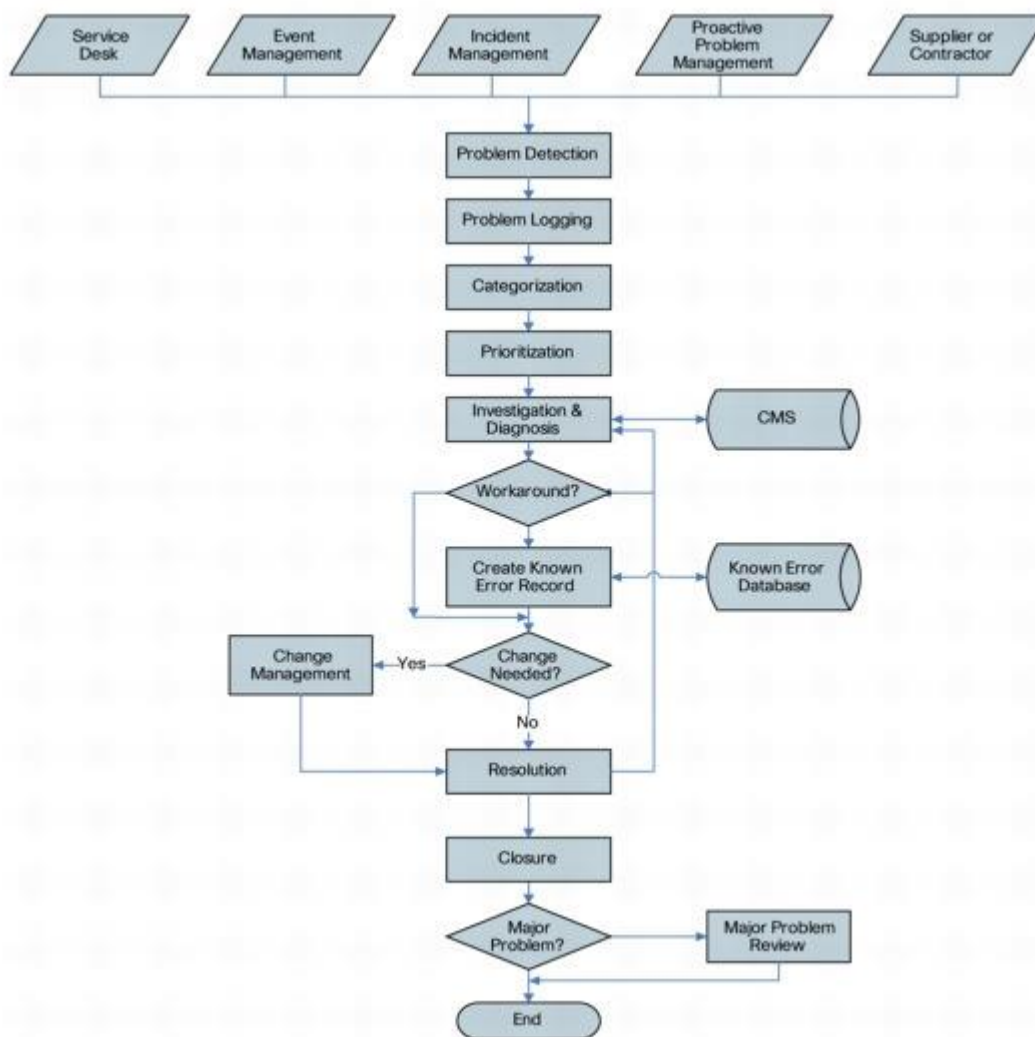
Анализ запросов (Процесс управления запросами)

Анализ изменений (Процесс управления изменениями)

Мониторинг событий и логов (Процесс управления Событиями)

Анализ релизов (Процесс управления Релизами)

Про-активная диагностика проблем (Процесс управления Проблемами)



Статусы проблемы:

Активный (In progress)

В ожидании (On pending)

Приостановленный (On hold)

Решена (Resolved)

Закрытый (Closed)

Классификация проблем по категориям (зависит от специфики организации, предпочтениям и т п):

Приложение / сервис

База данных
Аппаратное обеспечение

Определение групп разрешения проблем. Зависит от организационной структуры ИТ департамента, классификации проблем и т.п.

Результаты устранения проблемы:

Удачно выполненный (Successfully implemented)

Выполненный с незначительными проблемами (Implemented with Issues)

Частично выполненный (Partially implemented)

Не выполненный (Failed)

Определение метрик и показателей оценки эффективности и результативности процесса
Наличие временного решения проблемы (workaround)

Кроме элементов, выше указанных, необходимо также определить следующие элементы:
порядок информирования пользователя, сотрудника ИТ и менеджера проекта или супервайзера на различных этапах жизни проблемы.

Метрики соглашений

Связанные компоненты инфраструктуры, запросы, инциденты и т.п.

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Количество проблем

Количество проблем, связанных с аппаратным обеспечением

Количество проблем, связанных с программным обеспечением

Количество проблем, связанных с функционированием сети

Количество проблем по приложениям (сервисам)

Количество проблем, связанных с пользователями

Количество устранённых проблем

Количество проблем, устранённых в срок

Количество проблем вызванных инцидентами

Количество проблем вызванных событиями

Количество проблем вызванных запросами

Количество проблем вызванных изменениями

Количество повторных проблем

Количество проблем решённых с помощью «workaround»

Количество открытых проблем

Управление Доступами (Access Management ACM)

Процесс Управления Доступами является частью этапа «Сопровождения».

Управление доступом (Access Management) – процесс, отвечающий за допуск пользователей к использованию услуг, данных или других активов. Управление доступом помогает обеспечить конфиденциальность, целостность и доступность активов за счет того, что только авторизованные пользователи имеют возможность получить доступ или модифицировать активы. Основным драйвером процесса является процесс Управления информационной

безопасностью, так как именно он формирует политики и правила, которые реализуются процессом Управления доступом.

Данный процесс отвечает на такие вопросы как:

Формирование процесса управления Доступами.

Предоставление доступа пользователям к имеющимся сервисам

Предоставление доступа пользователям к информации

Утверждение процесса управления Доступами

Определение порядка взаимодействия с департаментом Безопасности

Управление доступом предоставляет ценность бизнесу благодаря тому, что:

каждый сотрудник имеет уровень доступа, необходимый для выполнения своих обязанностей;

контролируемый доступ к активам позволит организации поддерживать необходимый уровень конфиденциальности информации;

уменьшение вероятности ошибочных действий при работе с данными или использовании критичной услуги;

аудит использования услуг и отслеживание некорректной работы с ними;

быстрое лишение прав при возникновении необходимости;

может понадобиться для обеспечения соответствия требованиям регуляторов.

Деятельность по процессу:

Процесс управления Информационной Безопасностью

Процесс Управления Изменениями

Процесс Управления Событиями

Процесс управления Инцидентами

Процесс управления Запросами

Процесс управления Проблемами

Политика Информационной Безопасности

Формирование процесса управления Доступами

Классификация матрицы доступов

Предоставление доступов

Контроль за предоставлением доступов

Управление запросами доступов

Проверка

Предоставление прав и доступов

Мониторинг идентификации

Регистрация и мониторинг предоставления доступов

Изменение прав и доступов

Изъятие прав доступа

Участники процесса:

ИТ комитет

Сотрудники ИТ департамента

Представители Департамента Безопасности

Вводы процесса:

Процесс управления Информационной Безопасностью

Процесс управления Изменениями
Процесс управления Событиями
Процесс управления Инцидентами
Процесс управления Запросами
Политика Информационной Безопасности
Запросы

Выходы процесса:
Политики и процедуры предоставления доступов
Идентификация пользователей
Информация по пользователям

Показатели процесса:

Ключевые моменты процесса:
Департамент Безопасности является владельцем процесса
ИТ департамент управляет ИТ компонентами Информационной Безопасности

Процесс позволяет устранить такие проблемы в информационной безопасности как:
Высокий уровень инцидентов безопасности
Долгий срок предоставления доступов
Не прозрачность процесса предоставления доступов

Рассмотрим последовательность действий для предоставления доступа. Запрос доступа (или его ограничение) может быть осуществлен через следующие механизмы:
стандартный запрос от Отдела кадров (HR). Например, при найме нового сотрудника, увольнении, переводе в другой отдел и т. п.;
Запрос на изменение (RFC);
Запрос на обслуживание переданный рассмотренным выше процессом Управления запросами на обслуживание;
в процессе выполнения авторизованного сценария или опции (например, скачивание приложения с центрального сервера).
Верификация запроса на получение доступа включает в себя проверку двух категорий:
пользователь, запрашивающий доступ, действительно тот, за кого себя выдает;
пользователь, запрашивающий доступ, имеет право его получить;

Первый пункт проверяется обычно с помощью предоставления имени и пароля – они доказывают то, что пользователь является легитимным. В некоторых организациях могут быть использованы eToken, биометрическая аутентификация и т. п.

Идентификатор (Identity) – уникальное наименование, используемое для идентификации пользователя, человека или роли. Идентификатор используется для предоставления прав пользователю, человеку или роли. Примерами идентификации могут быть имя пользователя Иванов Иван или Роль «Менеджер Изменений».

Вторая категория требует некоторой независимой проверки, не связанной с запросом. Например,

- уведомление от Отдела кадров о том, что это новый сотрудник и ему необходим доступ к стандартному набору услуг;

- уведомление от Отдела кадров о том, что сотрудник получил повышение по службе и ему необходим доступ к дополнительным услугам;

- подтверждение от соответствующего процессу менеджера;

- предоставление запроса на обслуживание (с обоснованием) через сервис-деск;

- предоставление запроса на изменение через процесс Управления изменениями;

- политика безопасности, в которой оговорено то, что пользователи могут получить доступ к услугам, если они им необходимы.

Для новых услуг должны быть четко определены пользователи и группы, которые будут иметь к ним доступ.

Предоставление доступа. Управление доступом не принимает решений относительно того, кто и куда будет иметь доступ.

Процесс только реализует политики и правила, определенные на этапах Проектирования или Построения стратегии. После верификации пользователя, Управление доступом предоставит ему доступ для использования запрошенной услуги. В большинстве случаев непосредственное предоставление доступа требует действий со стороны каждой команды, поддерживающей услугу. Поэтому при проектировании услуг лучше предусмотреть автоматизацию процесса предоставления доступа.

Мониторинг статуса идентичности. Пользователи, работающие в организации, и их роли могут меняться. Примерами изменения могут быть:

- изменение обязанностей – в этом случае пользователю может понадобиться доступ к другому набору услуг или просто к дополнительным услугам;

- повышение или понижение в должности – в этом случае пользователю обычно необходим доступ к тому же набору услуг, но с другими уровнями;

- перевод – в этом случае пользователю чаще всего нужен будет тот же набор услуг, но в другом регионе и с другими данными;

- отставка или смерть – в этом случае все доступы должны быть немедленно аннулированы;

- выход на пенсию – в этом случае доступы либо аннулируются, либо ограничиваются. Например, сотрудник, вышедший на пенсию, может иметь доступ к услугам по покупке продуктов своей компании по сниженной цене;

- дисциплинарное ограничение – временное ограничение доступа пользователя из-за какой-то провинности;

- увольнение – в этом случае доступы должны быть немедленно аннулированы во избежание инцидентов безопасности.

Мониторинг доступа – Управление доступом ответственно не только за непосредственное предоставление доступа, но и за контроль его использования. Поэтому функция контроля доступа должны быть предусмотрена в рамках деятельности мониторинга. Если возникают какие-то нарушения, они характеризуются как инциденты безопасности. Управление доступом принимает участие в определении настроек систем обнаружения вторжений (IDS).

Отзыв или ограничение прав

Наряду с предоставлением доступа, Управление доступом ответственно за его аннулирование или ограничение.

Координация деятельности по системам обеспечения ИТ (IT Facility Coordination Management FCM)

Процесс координации деятельностью по управлению системами обеспечения ИТ сервисов является важным процессом в функционировании ИТ любой компании. Данный процесс отвечает на такие вопросы как:

- Организация процесса

- Разработка административных мероприятий по управлению системами сопровождения ИТ сервисов

- Организация работы ИТ документацией по управлению ИТ сервисами

Деятельность по процессу:

- Разработка и утверждение процессов управления ИТ сервисами

- Разработка и утверждение руководящих ИТ документов

- Разрешение конфликтов интересов

Входы процесса:

- Требования бизнеса

- Портфель сервисов

- Каталог сервисов

Выходы процесса:

- Подписанный протокол решения ИТ комитета

- Требования и рекомендации по вопросам систем обеспечения ИТ

- Подписанные руководящие документы по координации деятельности по системам обеспечения ИТ

- Контроль за исполнением требований по системам обеспечения ИТ

Участники процесса:

- ИТ Комитет

Показатели процесса:

- Удовлетворённость бизнеса

- Снижения количества инцидентов, вызванных сбоями в системах обеспечения ИТ

Ключевые моменты процесса:

- Как правило Административный департамент является владельцем процесса

- ИТ департамент обеспечивает управление процессом

Процесс: Координация деятельности по сопровождению ИТ сервисов (IT Facility Coordination Management FCM)

Назначение процесса (WHAT) и цели процесса (WHY):

Процедуры (HOW), Зона применения (WHEN) и Зона ответственности (WHO):

- Формирование требований и рекомендаций ИТ

- Обсуждение требований ИТ

- Принятие руководящих документов ИТ

- Ознакомление с руководящими документами ИТ

- Контроль за исполнением руководящих документов ИТ

- Внесение изменений в руководящие документы ИТ

- Разрешение конфликтов интересов

ЭТАП НЕПРЕРЫВНОГО УЛУЧШЕНИЯ СЕРВИСА (CSI Stage)

Введение

Непрерывное улучшение услуг (Continual Service Improvement или CSI) – постоянное улучшение услуг отвечает за управление улучшениями (совершенствованием) процессов Управления услугами и предоставления услуг. Производительность поставщика услуг постоянно

измеряется, и разрабатываются меры по улучшению процессов, услуг и ИТ-инфраструктуры с целью увеличения эффективности, результативности и эффективности затрат. Основной целью CSI является непрерывное «выравнивание» услуг в соответствии с изменяющимися требованиями бизнеса путем поиска и реализации возможностей улучшения услуг, которые поддерживают бизнес-процессы.

Цели и задачи:

- Формирование процесса непрерывного улучшения сервиса на всех этапах жизненного цикла.
- Формирование процесса мониторинга и измерений показателей сервиса.
- Проведение оценки и анализ достижения целей по уровням предоставления сервисов
- Организация деятельности по непрерывному улучшению процессов управления ИТ
- Оптимизация финансовой составляющей предоставления сервисов
- обзор, анализ результатов и формирование рекомендаций по улучшениям для каждого этапа жизненного цикла: Построения стратегии, Проектирования, Внедрения и Эксплуатации услуг;
- обзор и анализ полученных результатов на уровне услуг;
- поиск возможностей и осуществление соответствующей деятельности по увеличению качества услуг и результативности/эффективности процессов Управления услугами;
- увеличение эффективности затрат без негативного влияния на удовлетворенность заказчиков предоставляемыми услугами;
- использование подходящих методов управления для поддержки деятельности в рамках Непрерывного улучшения услуг.

Данная фаза определяется следующими процессами (2) улучшения сервиса (7 step improvement process):

- Управление процессом измерений (Service Measurement)
- Управление отчетностью (Service Reporting)
- Управление Улучшением Сервиса (Service Improvement)

Фаза непрерывного улучшения сервиса представляет из себя следующий цикл вопросов:

- Как мы движемся?
- Каково видение?
- Где мы сейчас?
- Где мы хотим быть?
- Как мы этого достигнем?
- Мы достигли желаемого?
- Как мы движемся?

«7 шагов по улучшению сервиса» включают в себя следующие действия:

- Сбор данных
- Анализ данных
- Определение «что может быть измерено?»
- Определение «что должно быть измерено?»
- Обработка данных
- Корректировка данных
- Предоставление и использование полученной информации

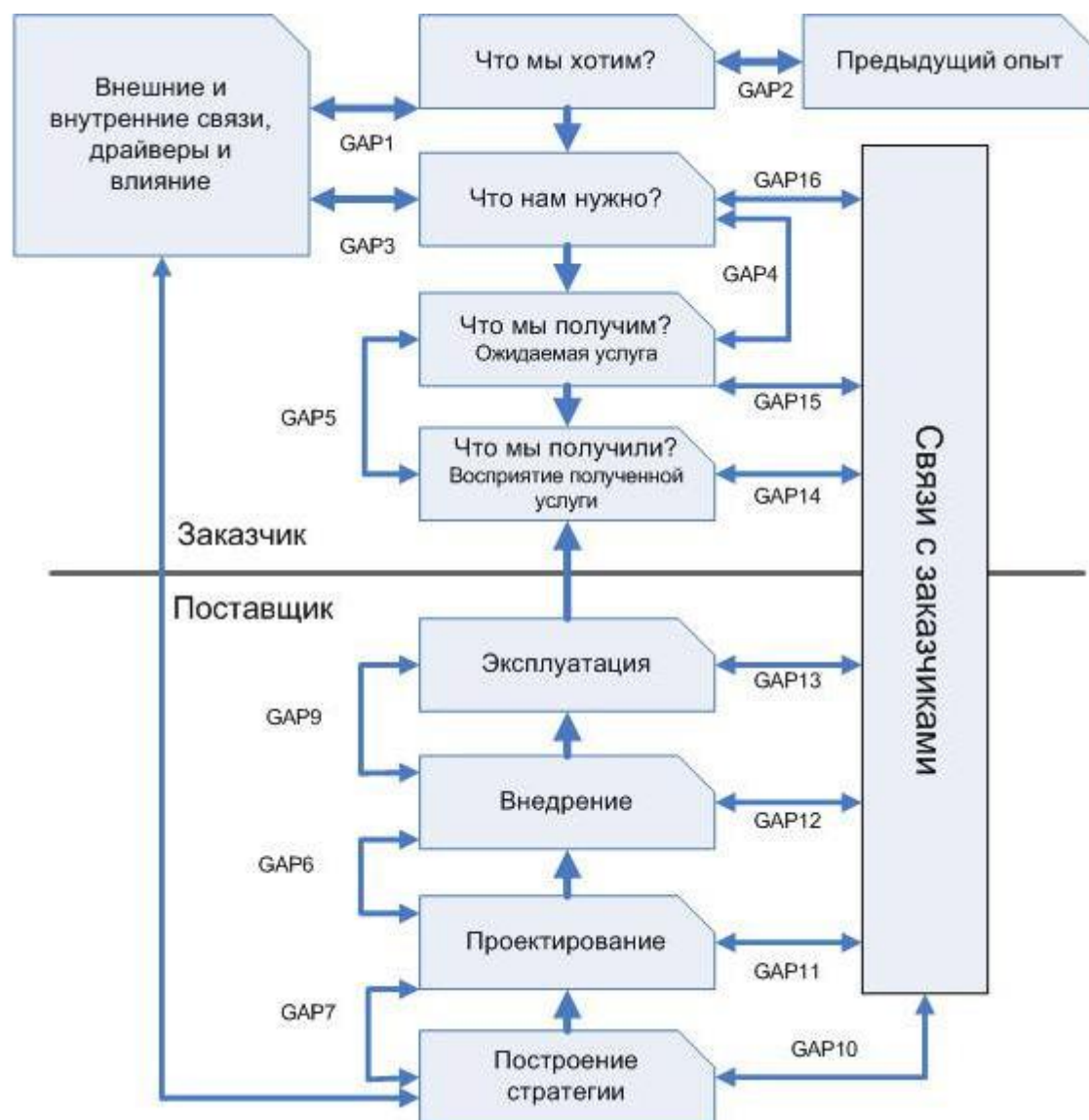
Возможности для улучшения услуг есть всегда. Процесс улучшения может быть сведен к шести шагам:

- понять и принять общую цель организации;
- оценить текущую ситуацию и получить объективную и аккуратную оценку того, в каком состоянии находится организация. Оценка базового состояния представляет собой анализ текущего состояния в контексте бизнеса, организации, персонала, процессов и технологий. Базовое состояние здесь обозначает собой некую отправную точку для измерения эффекта от реализации улучшений;
- расставить приоритеты улучшения на основе более глубокого анализа цели организации;

определить план CSI для процессов сервис-менеджмента;
 проверить метрики и системы измерения, которые позволят осуществить контроль в промежуточных точках реализации улучшений, измерить гибкость процессов и достижение приоритетов и целей бизнеса на уровне услуг;

в завершение, необходимо убедиться в том, что предложенные изменения реализованы, увеличение качества достигнуто и может быть сохранено в дальнейшем.

Улучшение не всегда можно объективно оценить. Кроме этого, у заказчиков и поставщиков услуг может сложиться разное отношение к улучшению. Чтобы уменьшить или предотвратить разрыв, необходимо информировать все заинтересованные стороны.



Результаты улучшения услуг можно определить следующими терминами
 улучшения – результаты, которые при сравнении с предыдущим состоянием могут показать увеличение желаемой или уменьшение не желаемой метрики.

выгоды – результаты, достигнутые в результате реализации улучшений, выраженные в финансовых терминах.

Возврат инвестиций – измерение разницы между выгодой, полученной от улучшения, и затратами на его реализацию.

Добавленная ценность от инвестиций – измерение ожидаемых выгод от инвестиций. Рассматривает как материальные, так и нематериальные выгоды. Нематериальные выгоды часто трудно поддаются оценке (улучшение репутации, удовлетворенности заказчиков и т.п.).

На практике, каждое улучшение должно быть доказано бизнесу со точки зрения ценности и необходимости. Можно выделить следующую деятельность по улучшению:

- увеличение финансовой выгоды
- улучшение качества бизнес операций
- увеличение продуктивности работы сотрудников
- улучшение непрерывности бизнеса
- улучшение взаимодействия поставщика услуг и заказчика;
- увеличение удовлетворенности пользователей
- увеличение качества и доступности услуг
- улучшение процессов планирования и закупок,
- улучшение процессов развертывания и реализации;
- улучшение управления информацией
- увеличение гибкости бизнеса
- улучшение соответствия целей ИТ и бизнеса;
- уменьшение негативного влияния ИТ на бизнес
- ИТ услуги проектируются для достижения конкретных требований;
- улучшенное распределение и использование ресурсов.
- инновационные выгоды
- внутренние выгоды ИТ-организации
- улучшенные связи, командная работа

Процесс улучшения в общем случае является частью глобального процесса улучшения организации в целом. Любое изменение организации является затратным и трудным процессом, встречающим на своем пути множество проблем. Основная проблема, как правило, связана с людьми, которые не любят изменения. Изменения в общем случае заставляют персонал отказываться от привычных практик работы.

Управление Измерениями (Service Measurement SMM)

Процесс Управления Измерениями является частью этапа «Непрерывного улучшения сервиса». Процесс предназначен для измерения метрик процессов для их последующей оценке и улучшения.

Данный процесс отвечает на такие вопросы как:
Формирование процесса управления Измерениями.

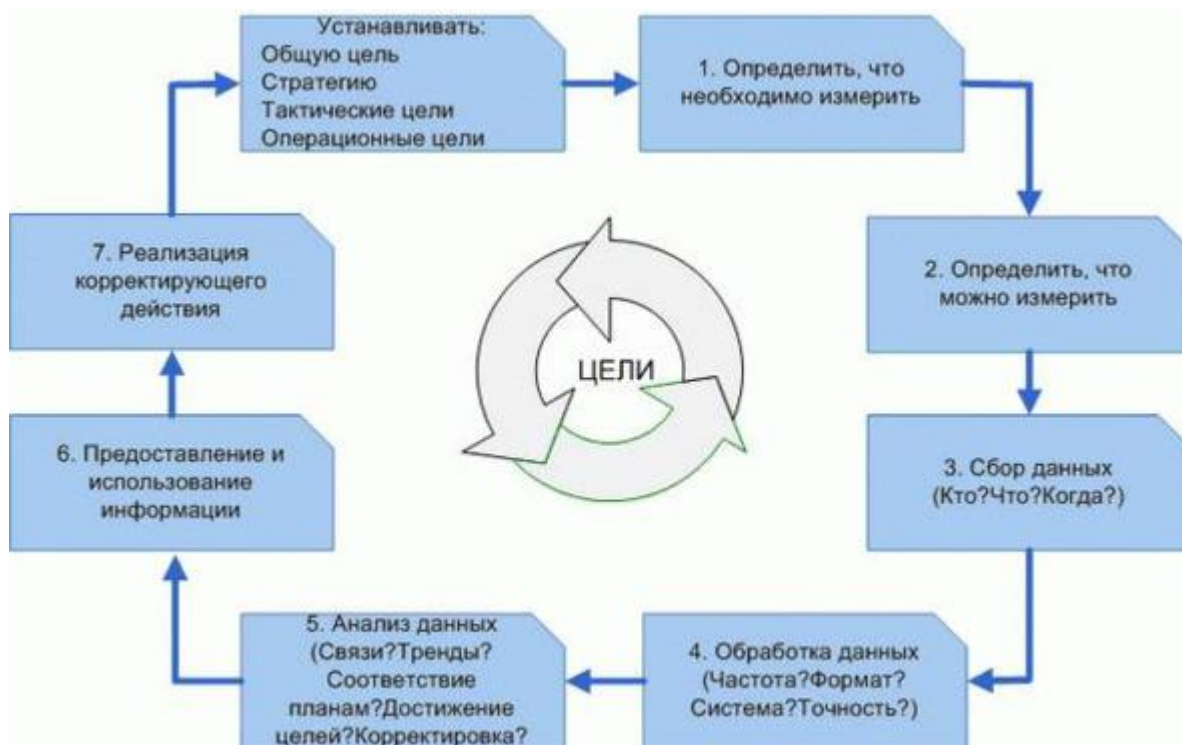
Деятельность по процессу:

- Утверждение процесса управления Измерениями
- Формирование процесса управления Измерениями
- Определение метрик доступности, надежности, производительности
- Формирование различных уровней измерений
- Установка метрик
- Анализ и интерпретация метрик и показателей

Входы процесса:

- Процесс Управления Изменениями
- Процесс Управления Событиями
- Процесс управления Инцидентами
- Процесс управления Запросами

Цели SLA
SLRs
OLAs
Contracts



Выходы процесса:
Программа улучшения сервисов
Метрики для процессов управления сервисами
Метрики и показатели для сервисов

Участники процесса:
ИТ комитет
Сотрудники ИТ департамента
Представители Департамента Безопасности
Представители бизнеса

Ключевые моменты процесса:
ИТ департамент является владельцем процесса

Используемая система измерения и соответствующие ей метрики должны отражать качество и эффективность процессов проектирования с точки зрения бизнеса, заказчиков и пользователей. Она должна достоверно показывать способность услуги удовлетворять согласованным требованиям бизнеса.

Есть четыре типа метрик, которые могут быть использованы для измерения производительности и возможностей процессов:

прогресс – измеренные в контрольных точках результаты процесса;

соответствие – соответствие процесса требованиям руководства и регуляторов.

результативность – аккуратность, корректность процесса, а также его способность достигать поставленные цели.

эффективность – мера целесообразности использования ресурсов для реализации процесса.

Для незрелого процесса лучше подходят первые две метрики, для зрелого процесса рекомендуется определять эффективность и результативность.

Кроме этого, существует четыре причины для измерения и мониторинга:

проверка – измерение и мониторинг проверяет принятые решения;

направление – измерение и мониторинг определяют направление дальнейших действий для достижения установленных целей;

обоснование – измерение и мониторинг позволяют создать обоснование тех или иных действий, построенное на реальных данных;

вступление – измерение и мониторинг позволяют определить точки, в которых необходимо осуществить коррекцию или изменения.

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Отчетность по Сервисам (Service Reporting SRM)

Процесс формирования Отчетов является частью этапа «Непрерывного улучшения сервиса». Данный процесс отвечает на такие вопросы как:

Формирование процесса предоставления отчетов.

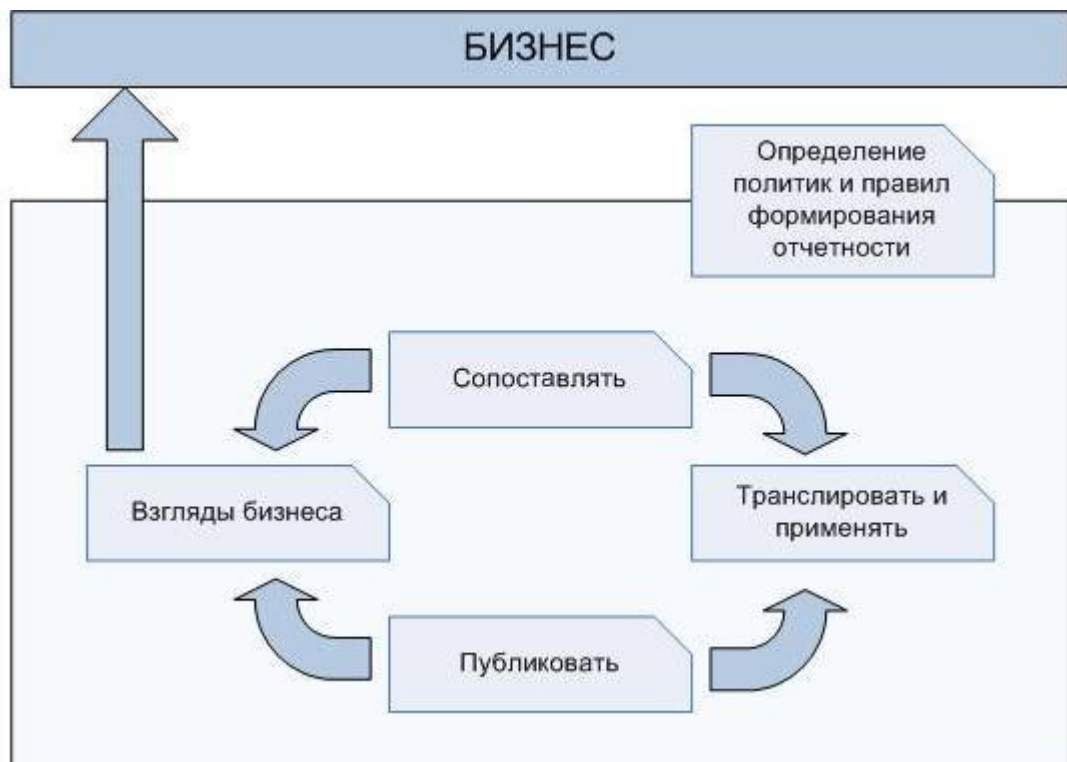
Деятельность по процессу:

Утверждение процесса формирования отчетов

Управление процессом предоставления отчетов

Определение измерений и метрик, включенных в отчеты

Определение групп и сервисов для предоставления отчетов



Входы процесса:

Процесс Управления Изменениями
Процесс Управления Событиями
Процесс управления Инцидентами
Процесс управления Запросами
Процесс управления измерениями

Выходы процесса:

Программа формирования отчетов
Отчеты по состоянию управления сервисами
Отчеты по состоянию сервисов

Участники процесса:

ИТ комитет
Сотрудники ИТ департамента
Представители Департамента Безопасности
Представители бизнеса

Ключевые моменты процесса:

ИТ департамент является владельцем процесса

При формировании отчетности ИТ необходимо:
определить цель отчета;

определить целевую аудиторию;
определить для чего будет использован отчет.

Значительное количество данных собирается в процессе ежедневной работы, но не все из них являются ценными и могут быть использованы для анализа и принятия решений. Для того чтобы структурировать процесс формирования отчетности необходимо согласовать политику и правила с бизнесом и этапом Проектирования. Они могут включать в себя:

- целевую аудиторию;
- соглашение о том, что будет измеряться и отражаться в отчетах;
- термины и границы;
- расписание формирования отчетности;
- доступ к отчетам и средства, которые будут использованы для его осуществления;
- расписание встреч для обсуждения отчетов.

Отчеты должны быть простыми для понимания и в то же время эффективными. Задачей ИТ является формирование отчетов в терминах, понятных бизнесу.

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Процесс Улучшения Сервиса (Service Improvement SIM)

Процесс Улучшения Сервиса является частью этапа «Непрерывного улучшения сервиса». Данный процесс отвечает на такие вопросы как:

Формирование процесса Улучшения Сервиса.

Один из важных критериев для организации это понимание стоимости улучшений и усилия, которые необходимо предпринять для их реализации. Эти значения должны сравниваться с выгодами, которые получит организация от улучшений. Выгоды посчитать гораздо труднее, чем издержки. Чтобы сравнивать затраты на улучшения и его результаты необходимо провести анализ и ответить, как минимум на следующее вопросы:

Какова стоимость простоя?

Какова стоимость повторного выполнения работ?

Какова стоимость излишней работы?

Какова стоимость проектов, которые не принесли ценности?

Какова стоимость задержки в предоставлении приложений?

Какова стоимость передачи инцидентов на вторую и третью ступень поддержки в сравнении с их разрешением на первой ступени?

Какова средняя стоимость часа работы для сотрудников?

В качестве методов измерения доступности и ведения соответствующих отчетов:

влияние потерянных минут – время простоя, умноженное на количество пользователей, на которых он повлиял. Пользователи в период простоя теряют свою производительность, так как не могут выполнять работу.

влияние на бизнес-транзакции – количество бизнес-транзакций, которые не могут быть завершены из-за простоя;

реальные издержки от простоя.

Деятельность по процессу:

Утверждение процесса улучшения сервисов

Цикл «Деминга» (PDCA)

Планирование (Plan)

Действие (Do)

Проверки (Check)

Реакция (Act)

Триггеры блокировки

Триггеры повторного запуска процесса

Входы процесса:

Все процессы управления сервисами

Процесс управления знаниями

Выходы процесса:

Программа улучшения сервисов

Внесение изменений в действующие процессы

Внесение изменений в действующие сервисы

Создание новых сервисов

Создание новых процессов

Оптимизация процессов

Оптимизация сервисов

Участники процесса:

ИТ комитет

Сотрудники ИТ департамента

Представители Департамента Безопасности

Представители бизнеса

Показатели процесса:

Удовлетворенность бизнеса

Улучшение показателей процессов

Улучшение показателей сервисов

Ключевые моменты процесса:

ИТ департамент является владельцем процесса

Критерии результативности – (KGI)

Критерии эффективности – (KPI)

Механизмы Контроля и Аудита ИТ

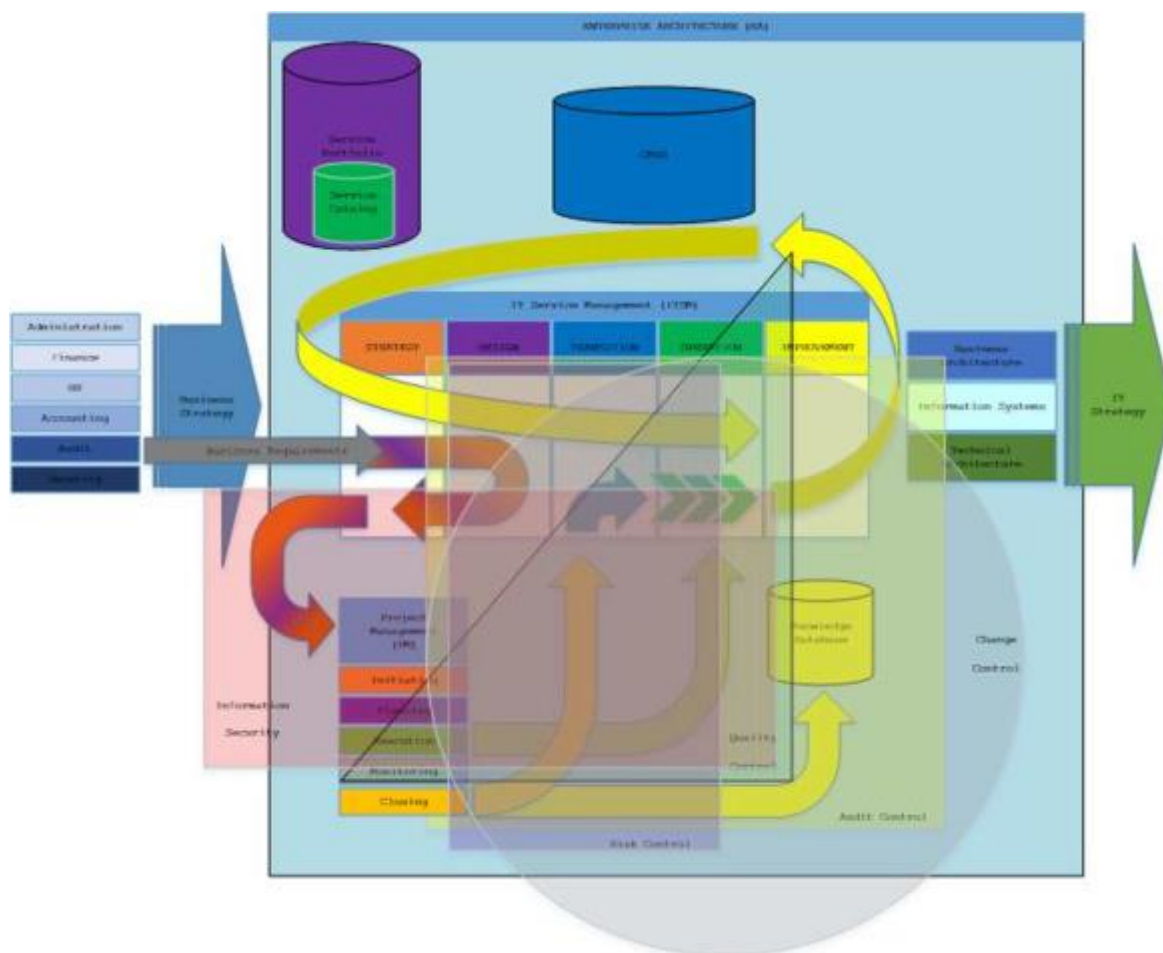
Общие Положения

Деятельность ИТ департамента имеет важное значение для организации. Как следствие необходимо принимать действия по ее контролю и аудиту активности. Как правило, данная функция возложена на департамент Внутреннего Аудита организации.

Основные задачи ИТ аудита:

Стратегические – соответствие целей и задач ИТ целям и задачам организации. Главная цель – результативность.

Оперативные – контроль за надлежащим исполнением регламента. Основная цель – эффективность.



Международные стандарты и практики ИТ аудита

«IT Audit Framework 2nd Edition» (ITAF) – международный стандарт проведения ИТ-аудита от организации ISACA. Действующая редакция выпущена в июле 2013 года. Целевая аудитория стандарта – специалисты в области ИТ-аудита. Стандарт предназначен для использования при проведении формализованных аудиторских проверок информационных систем и ИТ-инфраструктуры.

Стандартом определяются:

- основные термины и концепции, специфичные для специалистов в области ИТ-аудита;
- минимальные требования к навыкам и знаниям специалистов, выполняющих аудиторские проверки информационных систем;
- основные этапы проведения аудиторских проверок информационных систем и подготовки аудиторского отчета;
- перечень поддерживающих стандарт руководств, рабочих программ и инструментальных средств проведения аудита информационных систем.

Стандарт ITAF состоит из трех частей:

Общие стандарты – включает руководящие принципы для профессионалов в области аудита информационных систем: соблюдение независимости, объективности и профессиональной этики, поддержание знаний, компетенций и навыков.

Стандарты проведения аудиторских проверок – включает практики планирования и контроля аудиторских проверок, определение объемов работ в рамках аудиторских проверок, управление рисками и границами материальности, мобилизации ресурсов, управления проектом, практики сбора и хранение свидетельств аудита, использования методов экспертной оценки.

Стандарты отчетности – включает описание типов отчетов, средств представления отчетов и типов презентуемой информации.

Для каждой из частей стандарта ассоциацией ISACA разработаны руководства, рабочие программы и инструкции, поддерживающие проведение описанных аудиторских процедур. Руководства, рабочие программы и инструкции доступны на официальном сайте ассоциации. На момент написания статьи, стандарт ITAF является наиболее полным источником для специалистов в области ИТ-аудита, описывающим все этапы проведения проверки ИТ-систем и ИТ-процессов.

«Cobit 5» – руководство по проведению аудита в соответствии с COBIT v.5

Действующая редакция руководства выпущена организацией ISACA в июле 2013 года. Руководство предназначено для использования специалистами в области ИТ-аудита, ИТ-рисков и управления ИТ при проведении аудиторских проверок информационных систем в соответствии со сборником лучших практик COBIT 5. Составляющие:

- Детальное руководство по использованию COBIT 5 для организации и поддержания функции внутреннего ИТ-аудита в компаниях;
- Структурированный подход к проведению ИТ-аудита в соответствии с процессами и факторами (*enablers), описанными в COBIT 5;

В сравнении с ITAF, руководство «Cobit 5» обладает меньшей степенью формализации аудиторских процедур и более широким покрытием вопросов организации ИТ-процессов в соответствии с лучшими практиками.

«International Professional Practices Framework (IPPF) for Internal Auditing Standards»

Международный стандарт проведения внутреннего аудита от Института Внутренних Аудиторов (IIA). Целевая аудитория стандарта – сотрудники внутреннего аудита. Целью стандарта является определение:

- базовых принципов проведения внутреннего аудита;
- стандартного набора практик проведения внутреннего аудита;
- базовых показателей оценки эффективности процедур внутреннего аудита.

Несмотря на то, что стандарт не разрабатывался как стандарт ИТ-аудита, он определяет универсальные принципы и подходы, которые могут быть использованы, как при проведении внутреннего финансового и операционного аудита, так и при проведении внутреннего аудита информационных технологий. Для методологической поддержки стандарта в части проведения ИТ-аудита, ассоциацией IIA были разработаны детальные руководства по оценке ИТ-рисков (Guide to the Assessment of IT Risk) и аудиту информационных технологий (Global Technology

Audit Guide). Руководство «Guide to the Assessment of IT Risk» (GAIT) описывает взаимосвязь между бизнес-рисками, ключевыми контролями, встроенными в бизнес-процессы, автоматизированными контролями, критичными ИТ-функциями и Общими ИТ-контролями (IT General Controls). Руководство GAIT включает следующие публикации:

Методология GAIT (The GAIT Methodology) – описывает риск-ориентированный подход к определению и оценке Общих ИТ-контролей в рамках оценки управления системой внутреннего контроля необходимой для соответствия Статье 404 закона Сарбейнза-Оксли.

GAIT для оценки недостатков Общих ИТ-контролей (GAIT for IT General Control Deficiency Assessment) – описывает подход к определению критичности и материальности недостатков Общих ИТ-контролей, выявленных в рамках оценки соответствия Статье 404 закона Сарбейнза-Оксли.

GAIT для оценки бизнес и ИТ-рисков (GAIT for Business and IT Risk) – описывает шаги по определению ключевых ИТ-контролей, которые критичны для достижения бизнес целей и задач организации.

Руководство по аудиту информационных технологий «Global Technology Audit Guide» (GATG) состоит из 15 публикаций, описывающих процессы, процедуры и техники, используемые при проведении проверок информационных систем:

- ИТ риски и контроли (Information Technology Risk and Controls)
- Контроли в процессах внесения изменений и обновлений ИТ-систем (Change and Patch Management Controls)
- Процесс непрерывного аудита (Continuous Auditing)
- Управление процессами ИТ-аудита (Management of IT Auditing)
- ИТ-аутсорсинг (Information Technology Outsourcing)
- Аудит автоматизированных контролей (Auditing Application Controls)
- Управление доступом (Identity and Access Management)
- Управление непрерывностью бизнеса (Business Continuity Management)
- Разработка плана аудиторской проверки ИТ (Developing the IT Audit Plan)
- Аудит ИТ-проектов (Auditing IT Projects)
- Обнаружение и предотвращение мошенничества, связанного с использованием ИТ-технологий (Fraud Prevention and Detection in an Automated World)
- Аудит приложений, разработанных пользователями (Auditing User-developed Applications)
- Управление информационной безопасностью (Information Security Governance)
- Технологии анализа информации (Data Analysis Technologies)
- Аудит управления ИТ-функцией (Auditing IT Governance)

Детальность и бизнес-ориентированность данных стандартов, являются его сильными сторонами. Тем не менее, так как стандарт и поддерживающие руководства разрабатывались для использования специалистами не имеющими глубокого ИТ опыта, используемая терминология не всегда точно описывает технические аспекты проведения ИТ-аудита. Также некоторые руководства не обновлялись несколько лет.

Международные стандарты «ISAE N. 3402» и «SSAE N. 16»

«ISAE N. 3402» международный стандарт проведения аудиторских проверок сервисных организаций, разработанный международной организацией IAASB (the International Auditing and Assurance Standards Board), являющейся частью Международной Федерации Бухгалтеров (IFAC, International Federation of Accountants). Стандарт «SSAE N. 16» (ранее известный как SAS 70), выпущен ассоциацией AICPA (American Institute of Certified Public Accountants) и является адаптированной американской версией международного стандарта «ISAE No.3402». Целью стандарта «ISAE N. 3402» является предоставление унифицированного подхода к оценке эффективности системы внутреннего контроля сервисных организаций, в части подготовки достоверной финансовой отчетности.

PCAOB Auditing Standard No. 5 «An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements»

Действующая редакция стандарта разработана и выпущена организацией «The Public Company Accounting Oversight Board» (PCAOB) в 2007 году. Организация The Public Company Accounting Oversight Board (PCAOB) была создана законом Сарбейнза-Оксли в 2002 году как некоммерческая организация для контроля аудиторских проверок компаний, представленных на американских биржах, в целях защиты интересов инвесторов при подготовке независимого аудиторского заключения. Стандартом аудита PCAOB N. 5 «An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements» определяются требования по включению проверок ИТ-процессов и ИТ-систем в объем обязательных аудиторских процедур при проведении внешнего финансового аудита. Согласно стандарту, при проведении аудита контролей, связанных с подготовкой финансовой отчетности, аудитор должен получить понимание того, как используемые информационные системы и технологии оказывают влияние на процесс формирования финансовой отчетности. Аудитор также должен понимать какие контроли выполняются вручную, а какие реализованы на уровне информационных систем – автоматизированные контроли, в том числе как выполняются общие ИТ-контроли, которые важны для эффективной работы автоматизированных контролей. Эта информация должна быть учтена при оценке рисков искажения финансовой информации, обрабатываемой в информационных системах.

«ISO/IEC 27007: Guidelines for information security management systems auditing» и «ISO/IEC TR 27008: Guidelines for auditors on information security management systems controls»

Стандарты опубликованы международной организацией ISO/IEC в 2011 году. Целевой аудиторией стандартов являются специалисты в области информационной безопасности и ИТ-аудита, планирующие проведение compliance-аудита на соответствие требованиям стандартов ISO27001 и ISO27002. Цель стандартов – дать оценку соответствует ли организация/подразделение требованиям, изложенным в ISO/IEC 27001 и ISO/IEC 27002. Стандарты включают описание следующих аспектов аудита:

- Управление аудиторской проверкой.
- Непосредственное проведение аудита (планирование, проведение, ключевые активности, включая выборки и анализ, отчетность и последующий контроль исполнения).
- Управление командой аудиторов (поддержание компетенций и навыков, оценка членов команды).

Недостатком данных стандартов является отсутствие оценки рисков и последующей определением приоритетов контролей при планировании и проведении проверки. Тем не менее, стандарты удобны при подготовке к compliance-аудиту на соответствие стандартам ISO/IEC 27001 и ISO/IEC 27002.

Перечень контролей с применением COBIT v5

Control Objectives for Information and Related Technology (COBIT) представляет собой набор открытых документов, международных стандартов и руководств в области управления ИТ, аудита и информационной безопасности. Буквально на русский язык COBIT переводится как «Контрольные Объекты для Информационных и смежных Технологий», но в некоторых изданиях встречается более привычный для русского уха «Цели контроля для информационных и смежных технологий».

Основной целью COBIT является управление ИТ. Управление ИТ в свою очередь является неотъемлемой частью корпоративного управления. Корпоративное управление – комплекс управленческих решений и практик, применяемых высшим руководством с целью:

- определения стратегического направления;
- обеспечения достижения целей;
- адекватного управления рисками;
- эффективного использования корпоративных ресурсов.

Корпоративное управление и управление ИТ требуют баланса между целями, связанными с необходимостью соответствия требованиям и повышения эффективности, установленными высшим руководством. Ответственность за корпоративное управление лежит на Совете директоров и высшем руководстве.

В COBIT используется термин заинтересованные стороны. В первую очередь к ним относятся:

- Совет директоров и высшее руководство – определение направлений развития ИТ, оценка результатов и требования по исправлению недостатков;
- Руководители бизнес-подразделений – определение бизнес-требований к ИТ, обеспечение достижения пользы от ИТ и управление рисками;
- Руководство ИТ-служб – обеспечение и совершенствование ИТ-услуг в соответствии с требованиями бизнеса;
- Внутренний аудит и Служба внутреннего контроля – обеспечение независимой оценки, того, что ИТ предоставляет требуемые услуги;
- Управление рисками и Compliance – оценка соответствия нормативным документам с учетом рисков.

Основные принципы COBIT

Первый принцип COBIT – цели бизнеса и ИТ должны быть взаимосвязаны, но лидером этих «отношений» являются цели бизнеса, система контроля ИТ должна быть избирательной, то есть определять основные ресурсы ИТ и работать с ними; цели контроля должны быть четко определены.

Второй принцип COBIT – использование процессного подхода.

Определение целей, пожалуй, является одной из самых сложных и важных задач. В глобальном смысле руководство и менеджеры преследуют две цели – достижение поставленных бизнес-целей и предотвращение нежелательных событий (или исправление их последствий). Например, инвестирование средств в систему резервного копирования никак не поможет напрямую бизнесу, то есть не принесет ему непосредственной выгоды. Но оно сможет помочь в случае сбоя для быстрого восстановления информации и нормального функционирования. Другой немаловажный вопрос для руководства – где необходимы улучшения, сколько нужно в них инвестировать и как измерить результат? COBIT дает руководству ИТ методологию для поиска ответов на указанные вопросы. Ключевой составляющей управления ИТ является оценка процесса на основе предлагаемых COBIT моделях зрелости. Ресурсы ИТ используются для обеспечения и поддержки процессов ИТ. Процессы ИТ работают с корпоративной информацией и производят ее. Результатом цикла является соответствие корпоративной информации требованиям бизнеса.

COBIT выделяет следующие корпоративные требования к информации:

- полезность (результативность) – информация является значимой и имеет отношение к бизнес-процессам. Она получается регулярно, корректно, последовательно и в удобном виде;
- эффективность – информация получается посредством оптимального использования ресурсов;
- конфиденциальность – информация защищена от несанкционированного доступа и использования;
- целостность – исключено изменение информации субъектами, не имеющими на нее прав;
- доступность – субъекты, имеющие право доступа к информации, могут реализовывать его беспрепятственно;

•соответствие – информация соответствует законам, регулирующим актам и условиям контрактов.

•достоверность – руководству предоставляется вся необходимая информация для выполнения им своих обязанностей.

Еще одним ключевым понятием в COBIT является контроль.

Контроль (Control) – политики, процедуры, практики и организационные структуры, созданные для обеспечения разумной уверенности в том, что бизнес-цели будут достигнуты, нежелательные события предотвращены, а их последствия идентифицированы и исправлены.

Цель контроля (Control Objective) – для каждого процесса COBIT описывает одну высокоуровневую и несколько детальных целей контроля, являющихся, по сути, характеристиками «идеального процесса».

Практика контроля (Control Practice) – основной механизм контроля, поддерживающий достижение целей контроля за счет ответственного использования ресурсов, должного управления рисками и обеспечения соответствия ИТ целям бизнеса.

Методология контроля (Control Framework) – набор фундаментальных мер контроля, которые помогают участникам бизнес-процесса предотвратить финансовые и информационные потери организации.

Согласно рекомендации, COBIT v5 можно определить следующие ключевые этапы и контроли, а также возможные метрики показателей эффективности:

Оценка, Управление и Мониторинг (Evaluate, Direct and Monitor)

EDM01: Ensure Governance Framework Setting and Maintenance

EDM02: Ensure Benefit Delivery

EDM03: Ensure Risk Optimization

EDM04: Ensure Resource Optimization

EDM05: Ensure Stakeholder Transparency

Соответствие, Планирование и Оптимизация (Align, Plan and Optimization)

APO1: Manage the IT Management Framework

APO2: Manage Strategy

APO3: Manage Enterprise Architecture

APO4: Manage Innovation

APO5: Manage Portfolio

APO6: Manage Budget and Costs

APO7: Manage Human Resources

APO8: Manage Relationships

APO9: Manage Service Agreements

APO10: Manage Suppliers

APO11: Manage Quality

APO12: Manage Risk

APO13: Manage Security

Построение, Закупка и Внедрение (Build, Acquire and Implement)

BAI01: Manage Programmers and Projects

BAI02: Manage Requirements Definition

BAI03: Manage Solutions Identification and Build

BAI04: Manage Availability and Capacity

BAI05: Manage Organizational Change Enablement

BAI06: Manage Changes

BAI07: Manage Change Acceptance and transitioning

BAI08: Manage Knowledge

BAI09: Manage Assets

BAI010: Manage Configuration

Доставка, Обслуживание и Сопровождение (Deliver, Service and Support)

DSS01: Manage Operations

DSS02: Manage Service Requests and Incidents

DSS03: Manage Problems

DSS04: Manage Continuity

DSS05: Manage Security Services

DSS06: Manage Business Process Controls

Мониторинг и Оценка (Monitor, Evaluate and Assess)

MEA01: Monitor, Evaluate and Assess Performance and Conformance

MEA02: Monitor, Evaluate and Assess the System of Internal Control

MEA03: Monitor, Evaluate and Assess Compliance with External Requirements

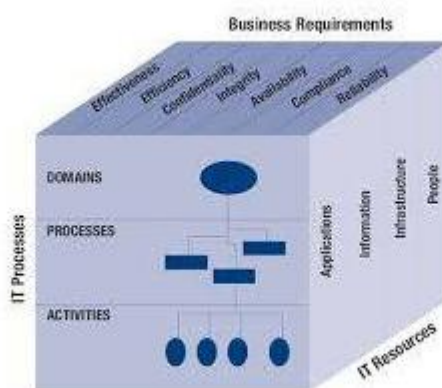
Принцип управления состоит из следующих цепочек действий:

Бизнес требования

Governance (EDM): – Оценка – Указание – Мониторинг состояния

Management: Планирование (APO) – Создание (BAI) – Сопровождение (DSS) – Мониторинг (MEA)

В отличие от версии 4.1 добавлены процессы управления рисками (Risk IT) и стоимостью (Val IT). Кроме этого изменена оценка показателей.



Бизнес Требования:

Результативность (Effectiveness) – ориентация на результат

Эффективность (Efficiency) – цена результата, КПД

Конфиденциальность (Confidentiality)

Целостность (Integrity)

Доступность (Availability)

Соответствие (Compliance)

Надежность (Reliability)

К ресурсам ИТ, согласно COBIT, относятся:

- приложения – прикладные системы и ручные процедуры для обработки информации;
- информация – данные в любой форме, введенные, обработанные и выведенные информационными системами в любой используемой бизнесом форме;
- инфраструктура – технологии и технические средства (аппаратное обеспечение, операционные системы, СУБД, сетевое оборудование), которые обеспечивают работу приложений.

•персонал – люди и их квалификация, необходимые для планирования, организации, приобретения, внедрения, работы, обслуживания, мониторинга и оценки информационных систем и ИТ-услуг. Персонал может быть внутренним и внешним.

Метрики контролей с применением COBIT v5

В данном разделе представлены возможные метрики для контролей.

Соответствие, Планирование и Оптимизация (Align, Plan and Optimization)

Возможные показатели:

Количество конфликтов в ответственности при обзоре распределения ответственности (segregation of duties)

Процент персонала, компетентного для выполнения своих обязанностей

Процент различия бюджета (выделенного к запланированному полному)

Процент ИТ бюджета, выделенного на оценку рисков

Процент ИТ функций, связанных с бизнесом

Процент ИТ инициатив и проектов, принятых бизнесом

Процент ИТ целей, напрямую соответствующих целям бизнеса

Процент ИТ сервисов, чья стоимость рассчитана и документирована

Процент ИТ сервисов, прошедших оценку соответствия качества (Quality Assurance)

Процент проектов, удовлетворяющих ожиданиям владельцев бизнеса

Процент проектов, соответствующих бюджету

Процент проектов, соответствующих срокам

Процент проектов, соответствующих заявленному качеству

Процент проектов, прошедших оценку после завершения

Процент проектов, с заранее рассчитанными показателями выгоды (ROI)

Процент резервных компонентов инфраструктуры

Процент повторного использования имеющихся элементов инфраструктуры в проектах

Процент повторных инцидентов

Процент ролей с документированными правами и обязанностями

Процент сервисов, не соответствующих утвержденной ИТ архитектуре

Процент сервисов, не соответствующих выбранной технологической платформе

Процент владельцев бизнеса, удовлетворенных качеством ИТ сервисов

Процент владельцев бизнеса, понимающих ИТ политики

Процент изменений, внесенных в операционные планы

Соотношение (актуального и запланированного) ИТ персонала и ИТ сервиса третьих сторон

Среднее соотношение управляемых ИТ департаментом и всех компонентов инфраструктуры

Задержка между обновлением стратегических и операционных планов

Частота обзора инфраструктуры и архитектуры на соответствие

Частота обзора механизмов контролей

Частота обзора со стороны управления и оценки рисков

Соотношение переработки сотрудников ИТ к регулярному рабочему времени

Построение, Закупка и Внедрение (Build, Acquire and Implement)

Возможные показатели:

Проблемы с приложениями, приведшими к видимым простоям

Ошибки или дефекты приложений в «рабочей» среде

Количество бизнес приложений (процессов) обслуживаемых «устаревшей» инфраструктурой

Количество различных технических платформ

Компоненты инфраструктуры более не поддерживаемые

Процент приложений с адекватным уровнем пользовательской и операционной поддержкой (обучением)

Процент времени, затрачиваемого разработчиками на сопровождение приложений

Процент изменений, внедренных без формального одобрения комитетом

Процент компонентов инфраструктуры, закупленных в обход установленных процедур

Процент владельцев бизнеса довольных поставщиками

Процент запросов на закупку, выполненных «предпочтительными» поставщиками
Процент проектов, выполненных в срок и установленный бюджет
Процент систем, не удовлетворяющих принятым техническим стандартам
Процент пользователей, удовлетворенных предоставляемой функциональностью систем
Количество «переделок», выполненных после внедренных изменений
Стоимость создания пользовательских материалов, процедур и т.п.
Удовлетворенность пользовательскими материалами, процедурами и т.п.
Сроки разработки и внедрения приложений
Разрыв по времени между изменениями, внесенными в инфраструктуру и обновление документации и обучения

Доставка, Обслуживание и Сопровождение (Deliver, Service and Support)

Возможные показатели:

Различия между документированным и текущим состоянием компонентов инфраструктуры
Количество инцидентов, связанных с физической безопасностью
Количество инцидентов, связанных с несоответствием с требованиями
Количество инцидентов, связанных с нарушением уровня доступа к инфраструктуре
Количество инцидентов, связанных с доступом к данным или их утечкой
Количество сервисных соглашений SLA с не соответствующим сопровождением, по отношению ко всем SLA
Количество часов обучения к количеству всего персонала
Нарушения в распределении прав доступа
Процент главных поставщиков, действия которых требует мониторинга
Процент приложений, не соответствующих требованиям политики паролей
Процент изменений в бюджете (план-факт)
Процент критических бизнес приложений (процессов), не покрываемых планом по управлению доступностью
Процент сервисов, не внесенных в сервисный каталог
Процент ИТ расходов, вызывающих вопросы со стороны бизнеса
Процент лицензий, закупленных, но не учтенных в конфигурационной депозитарии
Процент вне плановых отказов (доступности) сервисов в следствии инцидентов
Процент персонала, прошедших обучение по безопасности, обеспечению жизнедеятельности и т.п.
Процент запланированных работ, не выполненных в срок
Процент сервисов предоставляющих автоматическую отчетность (уровень автоматизации)
Процент сервисов реально измеряемые
Процент данных, успешно восстановленных
Процент систем и сервисов, не удовлетворяющих требованиям Информационной Безопасности
Количество запросов, выполненных не своевременно
Процент пользователей, не соответствующих требованиям политики паролей
Соотношение реальных операционных расходов к запланированным
Время простоя систем в следствии отказа физических компонентов инфраструктуры
Среднее количество часов обучения для ИТ персонала
Среднее время для восстановления единицы данных
Среднее время на между обнаружением несоответствия и его исправлением
Простои в следствии несоблюдения операционных процедур
Простои в следствии неадекватности операционных процедур
Частота (в днях) проведения оценки рисков
Частота (в днях) проведения распределения ИТ расходов
Частота (в днях) проведения тестирования резервных и архивных копий
Частота (в днях) обновления операционных процедур
Частота (в днях) обзора плана непрерывности бизнеса
Определение стоимости компонентов инфраструктуры за определённый период
Удовлетворенности пользователей уровнем доступности данных

Мониторинг и Оценка (Monitor, Evaluate and Assess)

Возможные показатели:

Количество выявленных (критических) инцидентов и не соответствий

Количество (важных) выявленных брешей в системе внутреннего контроля за определённых период

Количество действий по улучшению, выполненных в следствии мониторинга инфраструктуры

Количество нарушений политик и процедур

Количество инцидентов и проблем, вынесенных повторно на повестку ИТ комитета

Отчет по ИТ инфраструктуре выявленные со стороны внешних организаций

Уровень точности и полноты отчетов по ИТ инфраструктуре со стороны ИТ департамента

Процент критичных систем и процессов, находящихся под надлежащим наблюдением

Процент метрик, которые могут быть сравнимы с международными или индустриальными стандартами

Уровень усилий, затрачиваемых на сбор и предоставление информации и метрик

Стоимость штрафов и наказаний, за не соответствие требованиям

Частота предоставления отчетов ИТ комитету со стороны ИТ департамента

Частота проведения независимых обзоров или аудита

Время между нахождением несоответствий внутренним контролем и сообщения об этом

Удовлетворенность владельцев бизнеса уровнем мониторинга и контроля

Заключение

Как можно обратить внимание, аудит покрывает практически все аспекты деятельности ИТ, которые рассмотрены более детально в предыдущих главах. Поэтому не будет останавливаться на них подробно. Отметим лишь несколько важных моментов:

При проведении аудита, если вы находитесь на стороне того, кого проверяют, необходимо выяснить уровень проведения аудита, на уровне компании или департамента ИТ. Это важно потому, что не все процессы, происходящие в ИТ подконтрольны ИТ – ИТ не является владельцем процесса.

В новой версии CobiT 5 используется методика ISO 15504, на мой взгляд более правильная по сравнению со старой версией CobiT 4.1 использующей CMM. Новая методика объединила в себе помимо управления ИТ (Governance IT), управление инвестициями ИТ (Val IT) и управление рисками ИТ (Risk IT). Но и как результат комплексная оценка становится сложнее. Для примера: программа АСУ внедрена и работает. По старинке задаемся вопросом – документировано и контролируется, и есть возможность оптимизации – автоматизации. На оба ответа отвечает «да» (например, интеграция с системой «Б» проводится вручную, но реально документировано и контролируется). Оценка зрелости – «4». Все хорошо, но есть куда расти. Рекомендуются, выделяется бюджет, проект успешно внедрен. Автоматизирован. Ожидаем оценку зрелости – «5». По факту имеем: до внедрения за интеграцию отвечал конкретный исполнитель, занимало несколько минут, серьезная проблема за три года всего одна. Теперь, при сбоях интеграции – виновата «система», поиск причины обычно не приводит к результатам, а восстановление целостности данных – работа нескольких часов. На проект интеграции потрачены сотни тысяч. При новом методе оценки – прошлое состояние системы являлся приемлемым и оптимальным. Но чтобы правильно оценить процесс или систему в течении пары недель аудита – задача не тривиальная.

Так что совет для руководителя ИТ: не бойтесь спорить с аудитом и выражать свою точку зрения. Ваш опыт и знания по внедрению и сопровождению этой системы может быть уникален и вести к правильному решению.

Концепция Финансирования ИТ

Общие Положения

Определение стоимости предоставления ИТ услуги сложный процесс и зависит от стратегии и видения компании.

Экономическая эффективность – результативность экономической системы, которая выражается в отношении полезных конечных результатов ее функционирования к затраченным ресурсам. Складывается как интегральный показатель эффективности на разных уровнях экономической системы и является итоговой характеристикой функционирования национальной экономики. Внедрение и оценка эффективности ИТ проекта стандартными методами и подходами сложен по ряду причин.

Для понимания проблем введем определение двух видов организации:

- ИТ деятельность, является технологией основного производства. Справедливо для телекоммуникационных компаний, разработки и внедрения аппаратного и программного обеспечения, интернет провайдеров и т.п.

- ИТ деятельность является средством совершенствования и развития управленческой и производственной деятельности. К таким компаниям можно отнести предприятия производственного комплекса, банки, розничной торговли и т.п.

Модели финансирования ИТ

Модели финансирования ИТ можно разбить на следующие типы:

- «Красные» – стоимость расходов на ИТ распределяется пропорционально между компаниями без четкой фиксации. В расчет принимается лишь стоимость предоставления сервисов (service provisioning) – которая представляет из себя распределение расходов ИТ ресурсов.

- «Желтые» – ИТ департамент ведет учет стоимости расходов на ИТ для каждой компании на основе соглашения о предоставлении услуг. В расчет может приниматься как стоимость предоставления сервисов (service provisioning), так и стоимость сервиса (service value) – включающая в себя добавленную стоимость сервиса. Модель может представлять из себя соотношение $\text{стоимость сервисов} = \text{расходы на сервис}$.

- «Зеленые» – ИТ департамент ведет учет стоимости предоставленных услуг на ИТ для каждой компании на основе соглашения о предоставлении услуг. Департамент работает на полной самоокупаемости с возможностью генерирования добавленной стоимости. В данном случае понятия $\text{стоимости сервиса} = \text{расходы на сервис} + \text{добавленная стоимость}$.

Механизмы расчетов

Забегая вперед, рассмотрим механизмы расчетов. Для «Красной» модели, как правило используется «бюджетный» подход. ИТ бюджет формируется на основе двух составляющих:

- Общая стоимость расходов на сопровождение ИТ инфраструктуры
- бюджет ИТ проектов.

Как правило для руководства не имеет большого значения детализация распределения расходов по ИТ сервисам. На данном этапе бухгалтерии важно знать распределение расходов по плану счетов бухгалтерского учета: основные средства (материальные и не материальные), расходы за сервисы третьих сторон, фонд заработной платы. Бюджет ИТ проектов представлять из себя средства, выделенные ИТ департаменту на внутренние, «технические» проекты (лицензирование, обновление аппаратного обеспечения и т.п.), и средства, выделенные и контролируемые, из бюджетов бизнес подразделений в рамках «ИТ составляющей бизнес проектов». Как правило это самая простая модель.

«Желтая» модель характеризуется более высоким уровнем организации, но механизмы финансирования практически остаются такими же, как и в первом варианте. На данном этапе, ИТ предоставляет схему распределения ИТ расходов между бизнес подразделениями.

«Зеленая» модель подразумевает продажу ИТ сервисов, предоставление различных «пакетов» сопровождения, оплата по факту, фиксировано на ежемесячной, квартальной или годовой основе и т.п. Пакеты услуг могут быть определены как количественными (например, емкости хранения 100GB, 200GB и т.п.), так и качественными показателями (тип хранилища SSD, SATA и т.п.), а также готовыми шаблонами (M-size VM, S-size VM и т.п) виртуальных серверов. Это поможет в стратегическом планировании и оценке.

Модели ценообразования ИТ проектов

Модели финансирования задают параметры формирования стоимости ИТ проектов и сервисов. В качестве возможных моделей проектного ценообразования можно рассмотреть следующие варианты контрактов:

Контракт с «фиксированной ценой» (Fixed Price or Lump-Sum Contract)

Это традиционная модель проектной разработки, когда заказчик и менеджер проекта определяют в техническом задании весь объем работ, согласовывают фиксированный бюджет и точные сроки реализации проекта. В Fixed Price (или Fixed Fee) клиенты оплачивают конечный результат, а исполнитель – время своих разработчиков. В этом случае, если программисты проведут больше времени за разработкой, а бюджет не изменится, то прибыль компании снижается. Поэтому тут много зависит от умения менеджеров оценить заранее трудозатраты. Контракты с фиксированной ценой могут предполагать поощрения за достижение или улучшение отдельных параметров проекта, таких как сроки выполнения. Простейшей формой контракта с фиксированной стоимостью является заказ на покупку.

Контракт «Время и материалы» (Time & Materials T&M)

Это оплата заказчиком фактически затраченных ресурсов – времени разработчика. Данная модель несет гораздо меньше рисков для разработчиков (ИТ департамента или ИТ компании). Но и для заказчика имеет свои плюсы, когда высока степень неопределенности. Безусловно, важно определить предел рентабельности, чтобы были определенные рамки конечного бюджета.

Кроме этого могут использоваться и другие подходы к ценообразованию:

Контракт с возмещением затрат (Cost-Reimbursable Contract)

Тип контракта, подразумевающий оплату (возмещение) покупателем продавцу его фактических затрат, а также вознаграждение, обычно составляющее прибыль продавца. Затраты обычно подразделяют на прямые затраты и косвенные затраты. К прямым затратам относят расходы, непосредственно связанные с осуществлением проекта, такие как зарплата членов команды проекта. К косвенным затратам, также называемым накладными, общехозяйственными или административными расходами, причисляют затраты исполняющей организации на ведение бизнеса, отнесенные на проект, такие как зарплата сотрудников, косвенно принимающих участие в проекте, а также оплата потребленной офисом электроэнергии. Косвенные затраты обычно рассчитываются в процентах от прямых затрат. В контракты с возмещением затрат часто включают пункты с поощрениями или бонусами за достижение или улучшение отдельных параметров проекта, таких как сроки выполнения или общая стоимость.

Контракт с возмещением затрат плюс вознаграждение (Cost-Plus-Fee, CPF)

Тип контракта с возмещением затрат, при котором покупатель возмещает продавцу оговоренные затраты на выполнение работ по контракту, и продавец также получает вознаграждение, определяемое как оговоренный процент с затрат. Вознаграждение меняется в зависимости от фактической стоимости.

Контракт с возмещением затрат плюс вознаграждение за результаты (Cost-Plus-Incentive-Fee (CPIF) Contract)

По этому типу контракта с возмещением затрат покупатель возмещает поставщику оговоренные затраты (определяются условиями договора). При этом поставщик получает дополнительный доход при выполнении установленных критериев исполнения работы.

Контракт с возмещением затрат плюс фиксированное вознаграждение (Cost-Plus-Fixed-Fee (CPFF) Contract)

По этому типу контракта с возмещением затрат покупатель возмещает поставщику оговоренные затраты (определяются условиями договора) и уплачивает фиксированное вознаграждение.

Контракт с твердой фиксированной ценой (ФЦ) (Firm-Fixed-Price Contract, FFP Contract)

Тип контракта с фиксированной ценой, когда покупатель платит продавцу фиксированную сумму (в соответствии с условиями контракта), вне зависимости от затрат продавца.

Контракт с фиксированной стоимостью и вознаграждением за результаты (ФС+П) (Fixed-Price-Incentive-Fee (FPIF) Contract)

Тип контракта, когда покупатель платит продавцу фиксированную сумму (в соответствии с условиями контракта) и выплачивает дополнительную сумму при выполнении продавцом оговоренных критериев.

Вне зависимости от выбранной модели, важно иметь систему учета, которая показывает, каков общий бюджет, сколько уже сделано, какое количество часов при этом потрачено. Кроме этого особенности современного ИТ управления подразумевают сервисный и/или проектный подход к управлению. Особенности проектного учета, заключаются в том, что несколько разработчиков одновременно работают над несколькими разными проектами. Для обеспечения контроля, анализа и оценки необходимо внедрить системы учета временем и задач. Так же надо понимать, что применения количественных методов оценки и расчетов будет эффективно для ИТ с высоким уровнем зрелости, иначе можно получить обратный эффект.

Оценка эффективности ИТ проектов

На сегодняшний день существует два основных подхода к вопросу об экономической эффективности внедрения информационных систем.

В первом, наиболее распространенном случае экономическая эффективность оценивается весьма условно. Это происходит, когда в компании есть заказчик на стороне бизнеса, который четко понимает зачем ему нужен тот или иной ИТ-проект. Заказчик готов взять на себя всю полноту ответственности за эффект от его реализации. При этом до начала внедрения системы могут быть зафиксированы неизмеримые или сложно измеримые цели, например, повышение прозрачности бизнеса, улучшение управляемости или обеспечение единого информационного пространства и т. д. В этом случае оценить уровень подобных результатов, используя методы численной оценки, зачастую весьма непросто, и оценка может свестись к отражению высшим менеджментом своего отношения к реализованному проекту.

Во втором случае делаются попытки более формально с помощью количественных показателей оценить эффект от внедрения.

В качестве основных подходов в оценке ИТ проектов можно выделить следующие классические методы:

Портфельный подход – в компании имеется портфель ИТ проектов или ИТ инициатив. Справедлив для ИТ компаний, чей бизнес является предоставление, продажа решений, внедрений или консалтинга и т. п.

Бюджетный подход – финансирование ИТ происходит на основе выделения бюджета. Справедливо для организации, имеющей действующую ИТ структуру, основная функция которой представляет из себя сопровождение имеющейся ИТ инфраструктуры, и на нужды которой расходуется большая часть средств, порядка 70% процентов ИТ бюджета. Проекты носят не регулярный характер.

Проектный подход – наиболее современный подход к финансированию ИТ проектов. Предполагает выделение ИТ активности в законченный цикл (проект), с определением соответствующих показателей эффективности, как и в инвестиционных проектах:

- Срок окупаемости
- Возврат инвестиций
- Внутренняя рентабельность
- Чистая прибыль от проекта

Четкий учет и распределение времени по проектам дает возможность оценивать рентабельность проекта и повышает общую эффективность ИТ департамента. В качестве расчета рентабельности можно использовать метода начислений – то есть на основе признания доходов и расходов проекта, – независимо от фактического времени поступлений и выплат денежных

средств. Проектный учет методом начисления позволяет разбивать денежные потоки по отдельным задачам. В итоге становится видно, сколько каждый заказчик заплатил и какую долю он нам приносит в общей выручке. Причем важен не сам валовый доход, а чистая прибыль от конкретного проекта. Миллионный бюджет, десятки программистов и множество задач в сухих цифрах могут обернуться мизерной прибылью.

Оценка от внедрения, вне зависимости от подхода можно оценить в трех плоскостях:

- Расчетный эффект
- Эффект времени
- Специфический эффект

Расчетный эффект – оцениваются все финансовые метрики, как прямые, так и косвенные, затрагиваемые проектом до и после внедрения проекта (вплоть до использования туалетной бумаги). Сложный, но возможный подход, главное не переборщить.

Эффект времени – упор делается на расчет производительности труда в сравнении «до» и «после». Это может быть оптимизация процесса или деятельности, которая в конечном итоге приводит к экономии средств.

Специфический эффект – индивидуальный эффект, применимый к конкретной организации. В качестве примера можно привести повышения качества и времени предоставления информации, для принятия управленческих решений, без изменений «управленческой» модели принятой в данной организации.

Традиционно под эффективностью проекта подразумевается соотношение затрат и результатов проекта. Под затратами понимается совокупные затраты на приобретение, установку, настройку и поддержку программного обеспечения, а также расходы, связанные с приобретением и поддержкой требуемых технических средств, обучением персонала и т. д. Также в затраты могут включаться расходы, связанные с организационными изменениями, однако точно оценить их бывает проблематично.

Под результатами понимается тот эффект, который достигается при внедрении и последующей эксплуатации программного обеспечения. В некоторых случаях сложно сходу определить прямой эффект от проекта, будь то экономический или какой-либо другой. Классические методы оперируют «доходной» и «расходной» частью. Если для организаций первого вида, с моделей финансирования скорее всего «зеленой» все более или менее понятно, то для компаний второго вида все гораздо сложнее. С «расходной» частью оценки все относительно просто – ее можно рассчитать достаточно точно и однозначно. По поводу «доходной» части возникают вопросы. Например – проект внедрение информационной системы онлайн продаж. Если товары компании не продаются, то даже успешное внедрение проекта не повлияет, или повлияет незначительно на объем продаж. Или еще один пример, проект усовершенствования АБС (ABS) в банке поможет сократить время открытия счета на 30%. Эффективно, но если до внедрения два сотрудника в среднем открывали по десять счетов в день тратив на это порядка два-три часа (пятнадцать минут времени на каждый), то теперь они будут тратить не более двух часов. Остальное время сотрудника тратится в пустую.

Как видим, оценка ИТ проекта имеет свои нюансы, и в частности внедрение Информационной системы нужно оценивать, как «посредника» в достижении бизнес целей, а не как «двигатель». Основной упор делается на оценку:

- Соответствия бизнес целям.
- Рост производительности
- Экономия рабочего времени
- Эффективное управление персоналом
- Снижение стоимости операций

Для расчета эффективности ИТ проектов необходимо рассмотреть получаемый эффект по следующим направлениям:

•*Технический*. Определяется быстродействием выполнения производственных операций, машин, систем.

•*Экономический*. Определяется увеличением прибыли или снижением расходов.

•*Организационный*. Определяется степенью удовлетворения сотрудников и клиентов.

Существующие методы можно условно разделить на две группы в зависимости от используемого подхода к оценке:

Априорный подход – объединяет методы оценки и прогнозирования результатов внедрения информационной системы на этапе выбора решения и согласования объемов инвестиций. В данных методах используются прогнозные значения ключевых факторов, которые определяются на основании построенных моделей, при этом могут быть учтены различные виды рисков, влияющие как на эффекты, так и на затраты проекта внедрения информационной системы, а также различные неявные возможности. Наиболее привлекательны так как, позволяют оценить искомую эффективность до реализации самого проекта, на этапе технико-экономического обоснования. К ним относятся такие методы, как:

- оценка IRR (Internal Rate of Return),
- ROI (Return on Investment),
- TEI (Total Economic Impact),
- NPV (Net Present Value),
- BSC (Balanced Scorecard),
- EVA (Economic Value Added) и другие.

Методология оценки, основанная на опыте и эффекте внедрения систем в предыдущих проектах.

Проведение оценки в рамках данного подхода до начала реализации самого проекта, позволит ответить на вопрос, а стоит ли вообще инвестировать в данный ИТ-проект. Так, рассчитав рентабельность инвестиций и сравнив полученный показатель, например, со ставкой по банковским депозитам или с установленной в компании внутренней нормой доходности, в случае превышения первого над последним, можно говорить о том, что планируемые инвестиции будут эффективными.

Подход по факту – методы непосредственной оценки результатов внедрения информационных систем на этапе эксплуатации системы. Данные методы учитывают различные ключевые факторы до и после внедрения информационной системы и сравнение результата с затраченными усилиями на реализацию проекта внедрения системы. Суть подхода – сводится к сравнению планируемых и достигнутых результатов, которые имеются по всем заявленным целевым показателям. При этом точный результат изменений целевых показателей можно получить только в том случае, если известны их методика измерения и значения до внедрения системы. Основная проблема рассматриваемого подхода – это доказать, что изменения в компании, если они и произошли, связаны именно с внедряемой информационной системой, а не с тем, что, например, менеджмент компании начал принимать более эффективные решения вследствие изменения экономической конъюнктуры и т. д. При этом в компании могут параллельно внедряться несколько информационных систем, что еще более усложняет задачу оценки.

Методы оценки внедрения ИТ проекта можно условно разделить на следующие типы:

Финансовые (количественные) – Финансовые методы основаны на принципе дисконтирования, при этом ставка дисконтирования применяется как к потокам доходов, так и к потокам расходов. Дисконтирование – это определение стоимости денежного потока путём приведения стоимости всех выплат к определённому моменту времени. Дисконтирование является базой для расчётов стоимости денег с учётом фактора времени. Условно можно разделить на статические и динамические. Инструменты анализа, которые используются при финансовых методах:

- Чистый дисконтированный доход NPV
- Внутренняя норма доходности IRR
- Величина срока окупаемости проекта Payback Period,
- Индекс Рентабельности Инвестиций ROI.

Можно выделить два основных подхода при использовании финансовых методов: оценка величины прироста выгоды, т. е. рассчитывается разница между увеличением доходов, планируемыми к получению в результате эксплуатации ИТ-системы на протяжении некоторого

периода времени, и расходами на ее разработку, внедрение и эксплуатацию в течение этого же периода времени. И оценка чистого сокращения издержек, т. е. рассчитывается разница между ожидаемым сокращением издержек в результате внедрения ИТ-системы за определенный период (период окупаемости), и расходами на ее разработку, внедрение и эксплуатацию в течение этого же периода времени. Финансовые методы могут быть «статические» и «динамические».

Качественные – Качественные методы оценки, в методах данной группы предполагается дополнить количественные расчеты субъективными и качественными оценками, которые позволяют определить ценность персонала и процессов. Все они базируются на одной идее – целей, приоритетов и показателей по ним. В качестве методов используют:

- Метод информационной экономики (Information Economics) – объективная оценка портфеля проектов с направлением ресурсов туда, где они приносят наибольшую выгоду,
- Система показателей ИТ (IT Scorecard).

Опыт показывает, что, как правило, для качественной оценки этого достаточно.

Вероятностные – в этих методах используются статистические и математические модели, позволяющие оценить вероятность возникновения риска. В общем этих методов всего два:

- Прикладная информационная экономика (Applied Information Economics AIE)
- Справедливая цена опционов (Real Options Valuation, ROV)

Статистические – основаны на статистических данных,

Наиболее оптимальна комбинация методик с точки зрения полноты и минимизации затрат на проведение оценки в рамках априорного подхода:

Определение затратной части проекта с использованием метода Total Cost of Ownership (TCO). Для расчета TCO необходимо учитывать такие показатели, как:

- стоимость приобретения и поддержки оборудования, необходимого для работы системы в требуемом режиме;
- стоимость программного обеспечения и его поддержка производителем;
- стоимость внедрения программного обеспечения, которая включает в себя весь цикл создания продукта;
- стоимость дальнейшей поддержки реализованного продукта;
- стоимость обучения персонала, который будет работать с системой.

Определение эффектов от внедрения системы. Данная работа может состоять из нескольких компонентов:

•Прогнозирование эффекта от внедрения, исходя из результатов, достигнутых на ранее успешно реализованных аналогичных проектах в компаниях, принадлежащих к одному сектору экономики. Требуемые данные получаются исходя из анализа информации, обычно размещаемой разработчиками внедряемого программного обеспечения на официальных сайтах в виде пресс-релизов и отзывов своих клиентов, а также других открытых источниках. Однако, здесь кроются трудности, заключающиеся в том, что не всегда удается сразу найти требуемую информацию.

•Прогнозирование эффекта на основании оценок бизнес-заказчиков. В некоторых случаях можно привлечь бизнес-заказчиков и пользователей к оценке эффекта внедрения ИТ-системы. Это возможно в случае определенного уровня развития ИТ-культуры бизнеса компании, ответственности и наличия четкой постановки задачи со стороны бизнеса.

- Учет рисков, связанных с проектом внедрения.

Практическое применение данного подхода должно заключаться в построении многоуровневой детальной структуры «бизнес-стратегия – цели – задачи – подзадачи – функции/бизнес-процессы – ИТ-процедуры», которая свяжет несовместимые, на первый взгляд, характеристики и даст набор оценок эффектов совершенствуемой системы управления.

ИТ-задачи низкого уровня и ИТ-процедуры гораздо более стандартизируемы, чем цели конкретной компании. На похожести бизнес-процессов похожих компаний основан метод «прототипа», успешно используемый при внедрении сложных распределенных ИС. Суть его

заключается в изготовлении «единого эталона» и его дальнейшей «тонкой настройке» для нужд конкретного потребителя. Можно выделить состав обобщенных значимых направлений, которые называются «ключевые факторы экономической эффективности»:

- Минимизация упущенного дохода
- Формирование новых источников дохода.
- Снижение текущих эксплуатационных затрат.
- Снижение административно-управленческих затрат.
- Минимизация обязательных выплат.
- Снижение потребности в капитальных затратах.
- Увеличение оборачиваемости текущих активов.

Методы оценки эффективности ИТ проектов

Чистый дисконтированный доход (Net present value, NPV)

Этот показатель отражает непосредственное увеличение капитала компании.

$$NPV = \sum_{i=0}^n \frac{NCF_i}{(1 + Re)^i}$$

– NCF_i - чистый денежный поток на i -том интервале планирования
 Re - ставка дисконтирования

В том случае, если необходимо сделать выбор из нескольких проектов, предпочтение отдается проекту с большей величиной NPV. Величина чистого дисконтированного дохода рассчитывается как разность дисконтированных денежных потоков расходов и доходов, производимых в процессе реализации проекта за расчетный период. Для расчета необходимо знать величину первоначальных инвестиций, денежный поток от реализации инвестиций в определенный момент времени, шаг расчета (месяц, квартал, год) и ставку дисконтирования. Отрицательное значение NPV говорит о нецелесообразности принятия решения об инвестировании. Ставка реинвестирования, как правило, не высока, и расчет не приводит к большим ошибкам позволяет учесть то обстоятельство, что ставки дисконтирования со временем меняются.

Средняя норма доходности (Average Rate of Return ARR)

Показатель средней доходности инвестиций представляет собой отношение среднего за определенный период инвестирования притока денежных средств (например, средней чистой прибыли) к величине инвестированного капитала.

Индекс рентабельности инвестиции (Profitability index, PI)

Под этим показателем понимают отношение текущей стоимости денежного притока к чистой текущей стоимости денежного оттока с учетом первоначальных инвестиций. Если при расчете значение PI больше единицы, то проект следует принять, если меньше – отвергнуть. Критерий имеет значение при выборе проекта из нескольких с одинаковыми показателями NPV, но с разными объемами требуемых вложений.

$$\sum_{i=0}^n \frac{NCF_i}{(1 + IRR)^i} = 0$$

Внутренняя норма рентабельности (Internal rate of return, IRR)

Или внутренняя норма прибыли инвестиций – это значение ставки дисконтирования, при котором NPV проекта равен нулю. Расчет этого коэффициента необходим для того, чтобы определить максимально допустимый уровень расходов по проекту. Например, если проект финансируется за счет кредита от коммерческого банка, то IRR показывает верхнюю границу уровня банковской процентной ставки, превышение которой делает инвестиционный проект убыточным. Характеризует максимально приемлемый относительный уровень расходов, которые могут быть осуществлены при реализации определенного проекта. Показатель, определяющий относительный уровень этих расходов, называется стоимостью авансированного капитала является относительным показателем сопоставим с доходностью ценных бумаг и банковским процентом. Учитывает стоимость денег во времени и не зависит от ставки дисконтирования. Недостатки: Формула расчета IRR не имеет понятного определения, IRR показывает одинаковое значение в том случае, когда мы берем в кредит и когда даем займы. У проекта может существовать несколько значений IRR (при этом все значения могут быть неадекватны) или их может не быть вовсе. Преимущества: Простота расчета, Учет ликвидности проекта,

Модифицированная внутренняя норма рентабельности (Modified internal rate of return, MIRR)

Позволяет устранить недостаток внутренней нормы рентабельности, который может возникнуть в случае неоднократного оттока денежных средств, например, при долгосрочном строительстве объекта недвижимости. Реинвестирование в этом случае проводится по безрисковой ставке, величина, которой может быть определена на основе анализа рынка.

Дисконтированный срок окупаемости инвестиции (Discounted payback period, DPP)

Не имеет недостатков статического метода расчета срока окупаемости, поскольку учитывает стоимость денег во времени. В случае дисконтирования срок окупаемости увеличивается и проект, приемлемый по критерию PP, может быть неприемлемым по DPP. Определение периода окупаемости носит

вспомогательный характер относительно внутренней формы рентабельности или чистой текущей стоимости.

Индекс Рентабельности Инвестиций (Return of Investment ROI)

Это коэффициент возврата инвестиций, показатель рентабельности вложений. Он в процентном соотношении демонстрирует прибыльность (при значении больше 100%) или убыточность (при значении меньше 100%) конкретной суммы вложения денежных средств в определенный проект

$$ROI = \frac{NPV of Saving}{Investments} \times 100$$

Понятие ROI позволяет четко и на понятных принципах принимать управленческие решения. Поэтому в бизнесе – это один из самых востребованных показателей. Еще специалисты по информационным технологиям и внедрению программного обеспечения используют ROI в качестве инструмента, позволяющего оценить целесообразность внедрения того или иного программного продукта. Кроме того, ROI может использоваться в качестве начального инструмента при оценке инвестиционных проектов. Рассчитав показатель ROI, можно сопоставить его с доходностью вложения денежных средств в другие проекты или даже просто на банковский депозит. Поэтому, с помощью ROI можно отсеять проекты, которые не заслуживают дальнейшего внимания – попросту говоря, нецелесообразны. Вычисление ROI упускает из вида сегодняшнюю стоимость денег и риск, связанный с инвестицией. Для простых оценок эффективности вложений рисками и приведенной стоимостью денег (NPV) можно пренебречь. Для инвестиционных менеджеров ROI без учета рисков и приведенной стоимости проекта, может привести к неправильно принятым решениям.

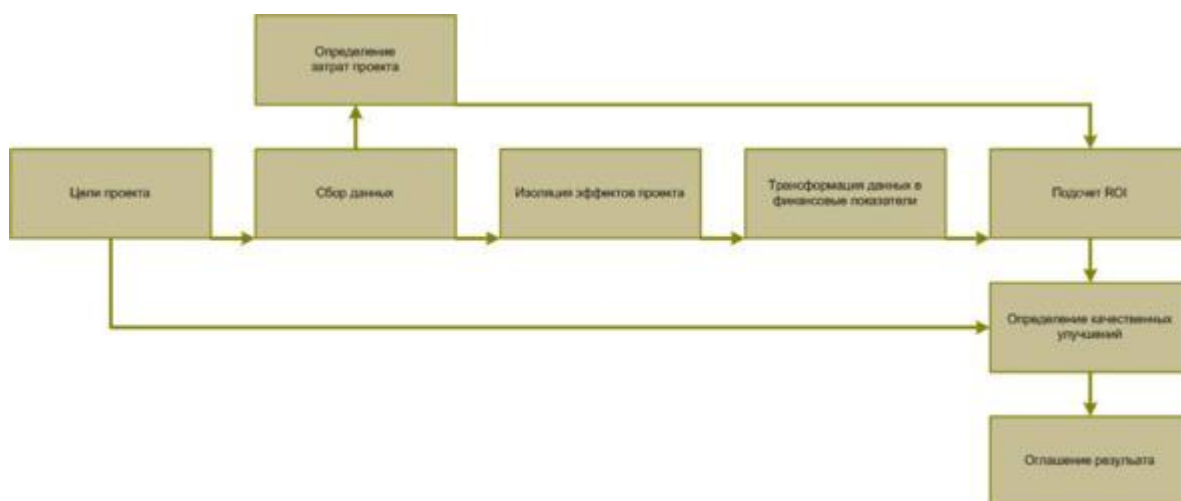


Диаграмма: Схема проектного ROI

Методология оценки, основанная на опыте и эффекте внедрения систем в предыдущих проектах

Данный метод можно отнести априорному подходу. Суть метода заключается в следующем: компании предлагается самостоятельно оценить ряд предложенных ключевых показателей ее деятельности. Затем полученные показатели сопоставляются с аналогичными показателями других клиентов из той же отрасли по имеющейся базе данных проектов или на основании информации из открытых источников. После этого компания получает оценку возможного экономического эффекта, который может быть достигнут в результате доведения ее ключевых показателей до сопоставляемого уровня в ходе реализации проекта. Таким образом, данный эффект оценивается не расчетным путем, а на основе результатов, достигнутых реальными компаниями в ходе реальных проектов. К достоинствам данного метода можно отнести простоту его использования. В то же время его недостатком является отсутствие гарантий того, что ранее достигнутый результат будет также достигнут этой компанией.

Экономическая добавленная стоимость (Economic Value Added, EVA)

Является достаточно простой методикой, суть которой состоит в вычислении разницы между чистой операционной прибылью предприятия и всеми затратами, понесенными предприятием на IT-инфраструктуру. Показатель EVA является постоянным индикатором для менеджеров: инвестируйте только тогда, когда прироста прибыли от капиталовложений достаточно для возмещения затрат на капитал.

Недостатки. Не отражает прогноз будущих денежных потоков. Показатель EVA определяется прибылью текущего год, что побуждает менеджеров к осуществлению проектов с быстрой отдачей и окупаемостью и не благоприятствует проектам, которые начинают давать отдачу позднее. Применять результаты данной методики можно лишь в динамике, т. е. рассматривая изменения величины показателя EVA с течением времени.

Совокупный экономический эффект (Total Economic Impact TEI)

С помощью методологии TEI компании могут продемонстрировать, обосновать и помочь понять осязаемую ценность проектов по внедрению информационных технологий руководству и главным акционерам. Если кратко, методология TEI состоит из четырех компонентов оценки инвестиционной стоимости:

- выгоды,
- расходы,
- риски
- гибкость.

«Стоимость» вычисляется по методике «Совокупная стоимость владения» (ТСО) и является единственной количественной оценкой данной методики. «Преимущества», «Гибкость» и «Риски» представляют собой качественные оценки. «Преимущества» позволяют судить о соответствии возможностей внедряемого продукта или компонента информационной системы требованиям проекта внедрения. Дополнительные возможности, которые появятся в работе сотрудников предприятия по итогам внедрения такого компонента или продукта должны быть оценены, как с точки зрения повышения эффективности работы, так и по их влиянию на выявленные операционные и технологические риски.

Недостатки: методика имеет достаточно узкий спектр применения. Ее можно использовать для анализа вариантов внедрения одного из компонента IT-инфраструктуры предприятия. Например, при выборе банком системы от разных производителей. Основной трудностью модели является непрозрачность определения прогнозных значений экономических выгод от внедрения, что является ноу-хау компании-разработчика данного метода.

Методология Быстрого экономического обоснования (Rapid Economic Justification REJ)

Методология экономической оценки, которая помогает организациям внедрять ИТ-решения в бизнес-процессы, а затем определять абсолютную финансовую прибыльность этих решений. Сущность методологии состоит в том, что она гарантирует, что инвестиции в информационные технологии определяются в соответствии с поставленными целями, важными для данной организации. Методология применяется к бизнес-процессам, в наибольшей степени влияющим на рост эффективности деятельности предприятия. Целью методологии является разработка бизнес-плана, который поможет главным менеджерам лучше понять достоинства конкретных вложений в ИТ. Модель REJ состоит из пяти шагов:

- оценка бизнеса,
- выработка решения,
- оценка прибыли и затрат,
- выявление и учет потенциальных рисков,
- расчет финансовых показателей.

По своей сути, методология REJ подобна методологии TEI и имеет схожие достоинства и недостатки. Кроме упомянутого выше, методология REJ помогает найти общий язык ИТ-специалистам и бизнес-менеджменту.

Достоинства: Взгляд на ИТ с точки зрения бизнес-приоритетов организации, стратегических планов ее развития, и основных финансовых показателей. Ключевой идеей методики является взгляд на ИТ с точки зрения бизнес-приоритетов компании, стратегических планов ее развития, и основных финансовых показателей (ROI и др.). Недостатки: Отсутствие учета временной стоимости денег и оценка проектов преобразования ИТ-инфраструктуры в целом.

Совокупная стоимость владения (Total Cost of Ownership, TCO)

Является наиболее эффективным механизмом мгновенной оценки общего объема затрат предприятия на ИТ-инфраструктуру. Методика TCO предусматривает оценку затрат на ИТ-инфраструктуру и на отдельные ее компоненты. Совокупные затраты включают как прямые или «бюджетные», которые берутся из бухгалтерских документов, так и «непрямые» – финансовые расходы, которые предприятие несет в виду неэффективности работы информационной системы и сервисных ИТ-служб. Эта методика является основой или составной частью значительного числа методик качественной и количественной оценки эффективности ИТ инфраструктуры предприятия. Достоинства: Позволяет четко выделить прямые затраты на ИТ. Недостатки: Не позволяет оценить дополнительные эффекты от использования ИТ и оценить риски использования ИТ или не использования

Система сбалансированных показателей (Balanced Scorecard, BSC)

Методика BSC разработана применительно к ИТ является качественным подходом к оценке эффективности как ИТ-инфраструктуры в целом, так и отдельного проекта внедрения. Основной упор делается на перенос и декомпозицию стратегических целей в планирование операционной деятельности и контроль их достижения. По сути это механизм взаимосвязи стратегических замыслов и решений с ежедневными задачами, способ направить деятельность всей компании (или группы) на их достижение

Система показателей ИТ (Balanced IT Scorecard, BITS)

Служит развитием методики BSC в сторону большей применимости для компаний, ключевые бизнес-процессы которых зависят от ИТ. Фактически, единственным изменением в данной методике, по сравнению с BSC, является дополнительная формализация показателей эффективности анализируемого процесса. В качестве таких показателей методика BITS рекомендует использовать следующие четыре:

- помощь в развитии бизнеса компании;
- повышение уровня сервиса, как для внутренних, так и для внешних потребителей;
- повышение качества принятия решений;
- повышение производительности труда. Спектр применения методики BITS практически совпадает с таковым для BSC.

Бюджет с нулевой базой (Zero-based budgeting)

Способ бюджетирования, при котором все расходы должны быть обоснованы для каждого последующего периода. В случае повышенной неопределенности и хозяйственной нестабильности своевременно принять решение о реструктуризации бизнеса исходя из максимально обоснованных финансовых расчетов и прогнозов, не продолжать финансирование тех проектов и программ, эффективность будущих результатов которых вызывают сомнения. В бюджеты, формируемые таким образом, не попадают ошибки, накопленные в предыдущих периодах. Достоинства: Затраты, рассчитанные в соответствии с данным методом, имеют большую степень обоснования. Руководители получают дополнительные возможности для обоснованного принятия решений о необходимости затрат или возможности их секвестирования (пропорциональное снижение государственных расходов). Основным недостатком являются большие трудозатраты. Продолжительность процесса планирования может во много увеличить время, затраченное при традиционном подходе. Затраты на использование данного метода могут превысить выгоды от его использования. Определение прогнозных значений некоторых показателей без использования базы прошлых периодов может быть менее эффективным или давать менее точный результат. В полной мере подход может быть использован только при достаточно высокой степени автоматизации.

Функционально-стоимостный анализ ФСА (Activity Based Costing, ABC)

Метод системного исследования функций объекта с целью поиска баланса между себестоимостью и полезностью, функционально-стоимостный анализ, в рамках которого выполняется дифференцированная калькуляция и распределение затрат на эксплуатацию системы по видам деятельности, продукции и функциям предприятия. Четкое ознакомление со стоимостью продукции дает возможность принимать верные стратегические решения по:

- назначению цен на продукцию;
- правильному сочетанию продуктов;
- выбору между изготавливать или приобрести;
- вложению средств в научно-исследовательские работы, автоматизацию процессов, продвижение и т. п.

Достоинства: Ясность в отношении выполняемых функций, за счет которой компаниям удается:

- уделить больше внимания управленческим функциям, таким как повышение эффективности дорогостоящих операций;
- выявить и сократить объем операций, не добавляющих ценности продукции.

Недостатки: Процесс описания функций может оказаться излишне детализированным, кроме того, модель иногда слишком сложна и ее трудно поддерживать. Часто этап сбора данных об источниках данных по функциям (activity drivers) недооценивается для качественной реализации требуются специальные программные средства. Модель часто устаревает в связи с организационными изменениями. Реализация часто рассматривается как ненужная «прихоть» финансового менеджмента, не достаточно поддерживается оперативным руководством.

Методика анализа поведения затрат (Costs Behaviors Analysis CBA)

Изучения зависимости изменений разных статей затрат от изменений объемов производства с целью классификации их на постоянные и переменные, предполагает детальное рассмотрение каждой статьи расходов по эксплуатации систем и является эвристическим методом, в котором используются экспертные оценки выгоды альтернативных вариантов инвестиционных вложений.

Метод SLCA (System Life Cycle Analysis)

Метод анализа жизненного цикла систем основан на сопоставлении положительных и отрицательных факторов функционирования корпоративной ИС.

Метод расчета совокупной ценности возможностей (Total Value of Opportunities TVO)

Используется для большей полноты отражения экономических результатов использования ИС.

Ключевые Показатели Производительности (Key Performance Indicators KPI)

Система оценки, которая помогает организации определить достижение стратегических и тактических (операционных) целей. Использование ключевых показателей эффективности даёт организации возможность оценить своё состояние и помочь в оценке реализации стратегии.

KPI – это инструмент измерения поставленных целей. Такая система позволяет руководству отслеживать в динамике эффективность деятельности каждого подразделения или сотрудника, возможность корректировки, прогнозировать результаты работы компании. Основное условие для объективности оценки и ее достижения – соблюдение правила SMART при установлении показателей. Они должны быть: конкретными (S), измеримыми (M), достижимыми (A), ориентированными на результат (R), ограниченными во времени (T). Недостатки: Высокие затраты на внедрения системы.

Пример оценки ИТ проекта

Рассмотрим практический пример расчета эффективности ИТ проекта на конкретном проекте. Автоматизированная Банковская Система (АБС) требовала постоянную связь между филиалом головным офисом для ведения бизнес деятельности. Не совершенство каналов связи, оборудования и внешние воздействия приводили к обрывам связи, что в свою очередь приводило к простому бизнесу, не выполнению планов и убыткам, и недополученной прибыли. На вопросы руководства, по невыполнению планов, представители бизнес подразделений всегда имели стандартную и универсальную отмазку: «... система не работает...». Председатель Правления банка и по совместительству куратор ИТ департамента, на одном из ИТ комитетов поставил вопрос на обсуждение. Уровень зрелости ИТ департамента, на то время был уже на высоком уровне, и ИТ комитету была предоставлена статистика (факты) по состоянию доступности каналов связи. В среднем на филиал приходилось порядка двух трех отключений в месяц в рабочее время (в течении одного часа). Кроме этого при увеличении времени задержки

в канале связи более 600 мс, АБС переставала адекватно функционировать. Показатель доступности каналов связи составлял в среднем порядка 93%-95% (полного времени доступности канала). Плохо это или хорошо? Приемлемо для бизнеса или нет? Какое из возможных технических решение применить? Анализ, проведенный бизнесом, позволил задать бизнес требования к проекту, а именно:

- Стоимость простоя филиала в час (филиалы были практически равноценные) приводил к невозможности выдачи десяти тысячного кредита. Возможности существующего обходного «ручного» метода снижал производительность выдачи почти в восемь раз.

- Скорость прием погашений по кредитам, падала почти в два – три раза.

- После восстановления связи, тратилось порядка двух трех часов для регистрации ручных операций в системе.

- Возрастал риск проведения операция, ошибок и потеря контроля. Кроме этого, ввод операций должен быть проведен до процесса «закрытия дня». В случае задержки, задерживалась работа всего банка.

Входные данные выглядят примерно так:

Количественные показатели:

Стоимость простоя 1 часа (в месяц) – 10,000.00

Стоимость простоя для 30 филиалов (в месяц) 300,000.00

Стоимость простоя для 30 филиалов (в год) 3,600,000.00

Дополнительные расходы (работники в месяц) 100.00

Дополнительные расходы (работники в год) 36,000.00

Упущенная прибыль и скрытые убытки (в год) 3,636,000.00

Упущенная прибыль (за 5 лет) 18,180,000.00

ИТ департамент рассмотрел возможные решения:

(1 филиал) 2км - 4 доллар/1 метр	1 год	2 год	3 год	4 год	5 год	Общие расходы
Подведение второго (медного) канала связи от второго провайдера на базе технологии ADSL						
Разовые расходы (установка, оборудование)	30,000.00	0	0	0	0	
Прокладка кабеля	240,000.00	0	0	0	0	
Ежемесячная оплата	43,200.00	43,200.00	43,200.00	43,200.00	43,200.00	
Общая стоимость решения	313,200.00	43,200.00	43,200.00	43,200.00	43,200.00	486,000.00
Подведение второго (медного) канала связи от второго провайдера на базе технологии SDSL						
Разовые расходы (установка, оборудование)	30,000.00	0	0	0	0	
Прокладка кабеля	240,000.00	0	0	0	0	
Ежемесячная оплата	61,200.00	61,200.00	61,200.00	61,200.00	61,200.00	
Общая стоимость решения	331,200.00	61,200.00	61,200.00	61,200.00	61,200.00	576,000.00
Подведение второго (оптического) канала связи от второго провайдера						
Разовые расходы (установка, оборудование)	30,000.00	0	0	0	0	
Прокладка кабеля	720,000.00	0	0	0	0	
Ежемесячная оплата	180,000.00	180,000.00	180,000.00	180,000.00	180,000.00	
Общая стоимость решения	930,000.00	180,000.00	180,000.00	180,000.00	180,000.00	1,650,000.00
Обеспечение второго канала связи на базе провайдера мобильной связи						
Разовые расходы (установка, оборудование)	30,000.00	0	0	0	0	
Ежемесячная оплата (1 филиал)	324,000.00	324,000.00	324,000.00	324,000.00	324,000.00	
Общая стоимость решения	354,000.00	324,000.00	324,000.00	324,000.00	324,000.00	1,650,000.00
Внесение изменения в код программы, предоставляя возможность ведения «off-line» операций						
Резонжиринг АБС	400,000.00	0	0	0	0	
Общая стоимость решения	400,000.00	0.00	0.00	0.00	0.00	400,000.00
Увеличение скорости канала связи первого провайдера						
Разовые расходы (установка, оборудование)	0.00	0	0	0	0	
Ежемесячная оплата	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	
Общая стоимость решения	54,000.00	54,000.00	54,000.00	54,000.00	54,000.00	270,000.00

Стоимость контрмер

ИТ отсеял следующие решения: Не смотря на явное финансовое преимущество «Внесения изменений в код программы» – качественные показатели решения: Потребуется внесение изменений в бизнес процессы банка и исходя из опыта работы с данной командой разработчиков – сроки и возможности не определены. Увеличение скорости текущего соединения (второе по эффективности) – не решало проблем с провайдером, провалы в качестве связи. Решения «второго провайдера на базе мобильной связи»: несмотря на отсутствие необходимости в прокладке кабеля, что ускоряло внедрение решения, имеет недостатки: высокая стоимость ежемесячного платежа – порядка 900 манат и отсутствие возможности по увеличению скорости в дальнейшем (не более 256 кбит/сек). Наиболее приемлемые решения были предоставлены на ИТ комитете: Использование второго провайдера с использованием оптики, выделенного канала или ADSL соединение (на основе медного кабеля). Стоимость прокладки оптического кабеля, на тот период составляла порядка 10—12 манат за погонный метр. Средняя удаленность филиалов от АТС составлял порядка 2—3 километров. Кроме этого требовалось покупать более дорогое оборудование. Стоимость ежемесячной оплаты составлял порядка 500 манат. Ситуация усугублялась тем, что не во все районы можно было провести оптический кабель как «последняя миля», а также отсутствие специалистов и оборудования в районах, способных оперативно восстановить обрыв оптического кабеля.

Приоритетное решение на базе второго провайдера с использованием выделенной линии или ADSL (что в конечном случае и было выбрано) обеспечивало требования: стоимость ежемесячной оплаты ADSL была на 40% ниже (порядка 120 манат) при средней скорости выше вдвое. Не требовало дорогостоящего оборудования, прокладка медных каналов связи порядка четырех манат на погонных метр. Возможности увеличения скорости в дальнейшем. Максимальная утилизация имеющегося оборудования. Время внедрения и восстановления обрыва быстрее. Дешевле в финансовом плане по сравнению с тем же решением с технологией SDSL. Дополнительная настройка сетевого оборудования позволяло использовать следующую модель:

- В штатном режиме по основному каналу связи (медная пара, синхронная выделенная линия скорость 128 кбит/сек) гонялся трафик ключевых ИТ сервисов, удаленной поддержка и АБС. По второстепенному каналу (медная пара, асинхронная линия скорость 256/128 кбит/сек) проходил второстепенный трафик – интернет, почта и т.п.

- При отказе одного из каналов «важный» трафик переключался на второй канал автоматически, второстепенный трафик проходил по остаточному принципу. Финансовые показатели расчета эффективности проекта (по формулам, приведенным ранее в данной главе) показывают высокую рентабельность, быструю окупаемость решения, чуть более года, даже при самых не благоприятных сценариях. Быстрый возврат инвестиций. Качественные показатели – разделение важного и второстепенного трафика.

После реализации были получены фактические показатели, как технические – суммарное время доступности каналов связи порядка 99.7%, скорость основного канала связи не менялась, увеличение со временем скорости «более дешевого» канала связи в два раза не значительно увеличило операционные расходы. Оборудование основного канала связи использовалось на протяжении десяти лет. Дальнейшее развитие технологий связи, снижение стоимости оптических каналов связи и повышение требований к пропускной способности каналов позволил постепенно перевести «основной» канал связи на оптический.

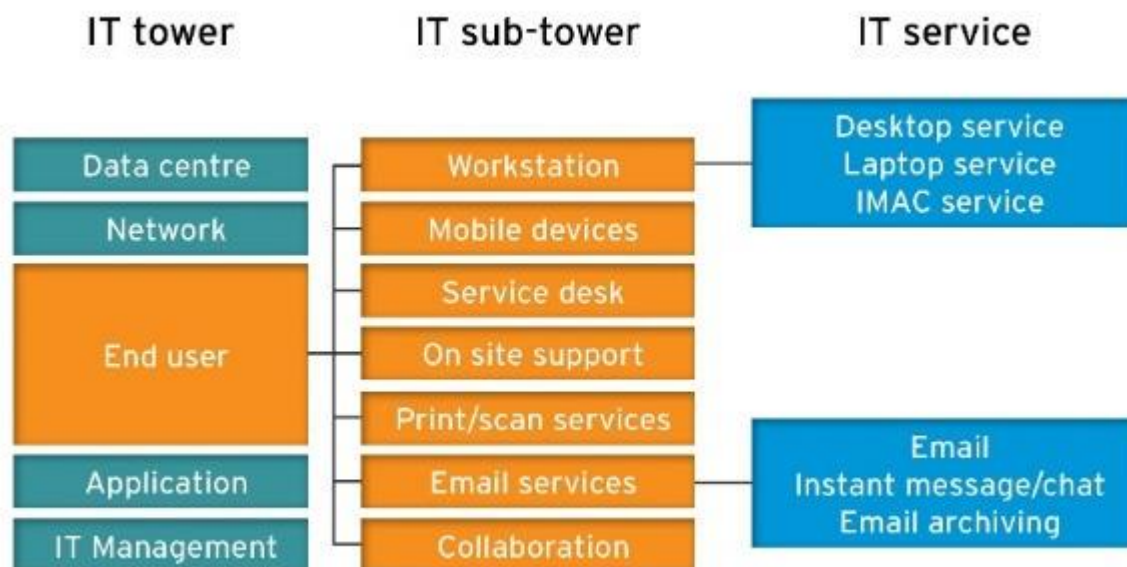
Из практики проведения ИТ проектов, могу отметить, что для внутренних проектов, крайне редко приходилось использовать количественные финансовые показатели. Во многом причина была в отсутствии входных финансовых показателей со стороны бизнеса и задачи, поставленные перед ИТ, сложно было выразить в финансовых или количественных показателях. Тем не менее это полезно знать и по возможности применять.

Формирование стоимости ИТ сервисов

Теперь рассмотрим частный случай ИТ проектов, с которым приходится сталкиваться ИТ директорам, расчет стоимости внедрения и сопровождения ИТ сервисов.

Стоимость (Cost) – Денежное выражение, или цена, операций проекта или элементов, включающее цену (в денежном выражении) ресурсов, необходимых для выполнения

и завершения операции или элемента, или для изготовления элемента. Конкретная стоимость может быть составлена из стоимости элементов, включая прямые трудозатраты, другие прямые затраты, косвенные трудозатраты, другие не прямые затраты и цену закупки. Необходимо различать понятия расходы и стоимость.



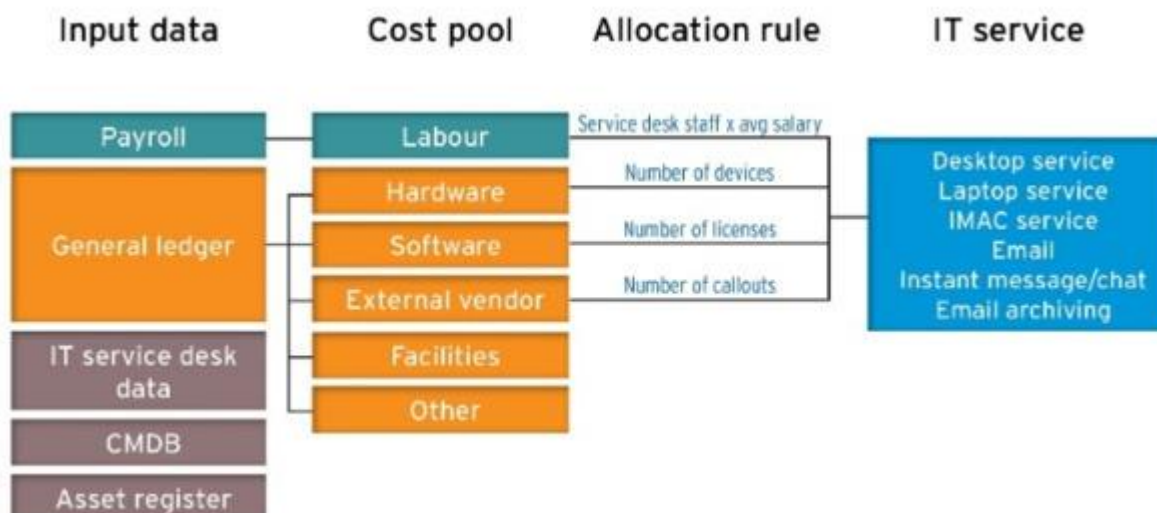
Для формирования стоимости предоставляемых услуг, необходимо ввести следующие понятия:

Прямые затраты – затраты, которые, могут быть прямо и непосредственно отнесены на конкретный вид сервиса.

Косвенные затраты – затраты, которые, в отличие от прямых затрат, не могут быть напрямую отнесены на себестоимость сервиса. Косвенные затраты обычно распределяются пропорционально между различными видами сервисами по определённой базе.

Переменные затраты – виды расходов, величина которых изменяется пропорционально изменению объемов использования сервиса.

Постоянные затраты – представляют собой затраты, которые не зависят от объёма использования сервиса, противопоставляемые переменным затратам, с которыми в сумме составляют общие затраты.



Выделенные ресурсы (Dedicated Resources) – вычислительные мощности закреплены за определенной организацией. Например, сервер для обмена файлами (файловый сервер), который используется только данной организацией. В этом случае все стоимость вычислительных ресурсов переносится на организацию. Справедливо для компаний холдинга или предоставляющим ИТ сервисы.

Разделяемые ресурсы (Shared Resources) – вычислительные мощности используются совместно различными организациями. Например, почтовый сервер, который используется различными организациями. В этом случае, стоимость вычислительных ресурсов распределяется между организациями. Механизмы распределения могут быть следующие:

- Фиксированные
- Пропорциональное распределение по организациям с полным покрытием стоимости.
- Пропорциональное распределение по использованию
- Прочие варианты

Методы и подходы формирования стоимости ИТ сервиса

Для формирования стоимости ИТ сервисов, необходимо определить следующие понятия, используемые в расчетах для формирования стоимости это:

Стоимость сервиса – совокупная стоимость компонентов сервиса, без учета клиентских доступов. Так, например, сервис активного каталога включает в себя стоимость вычислительных ресурсов и лицензии на операционную систему. Как правило лицензирование ИТ решений состоит из стоимости серверной части и стоимости лицензий на пользователя или устройство. Первую часть лицензирования можно принять как «фиксированные» расходы – например один сервер Активного Каталога может обслуживать до пяти тысяч пользователей или устройств.

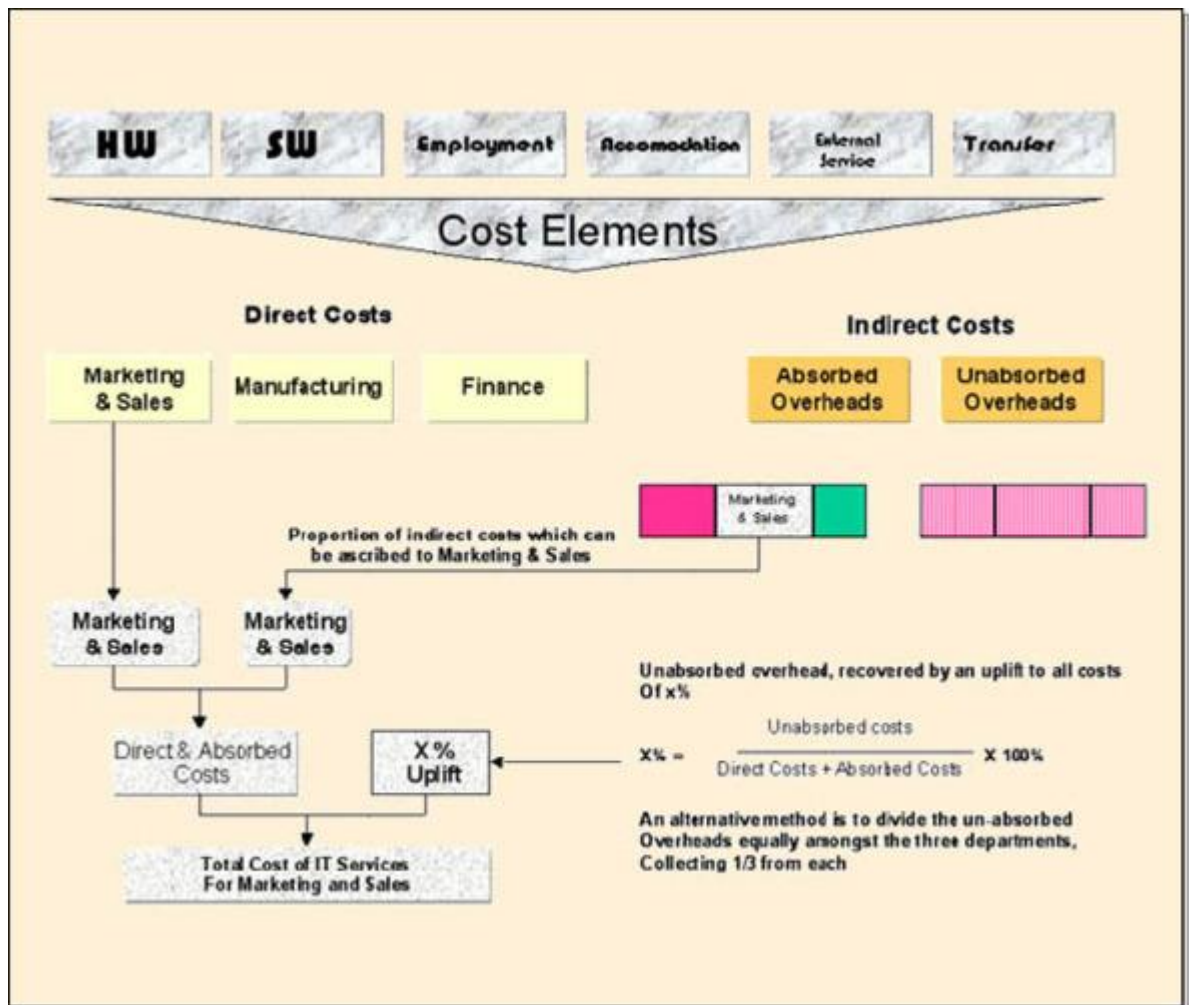
Стоимость доступа – стоимость лицензий для доступа клиентов к сервису (например, Windows CAL, Exchange CAL и т.п.). состоит из стоимости лицензий на пользователя или устройство. Стоимость доступа необходимо принять как «переменные» расходы. Сколько пользователей используют данный сервис – на столько возрастает стоимость использования сервиса.

Стоимость сопровождения сервиса – стоимость расходов времени сотрудников ИТ департамента на выполнение регламентных работ по сопровождению сервиса. В зависимости от типа организации, модели финансирования, необходимости в точности расчетов, может включать в себя стоимость внедрения сервиса, необходимые ресурсы тестовых и эталонных площадок, сервисов обновления, время сотрудников ИТ департамента по проектированию сервиса, стоимость средств мониторинга и т.п.

Стоимость поддержки пользователей – стоимость работы со стороны ИТ департамента по поддержке пользователей. Формируется в основном по количеству времени, затраченному сотрудниками подразделения Поддержки Пользователей. Может включать в себя стоимость средств управления инцидентами, запросами и т.п. Кроме этого зависит от времени реакции (соглашение об уровне предоставления сервиса) и исполнения запросов.

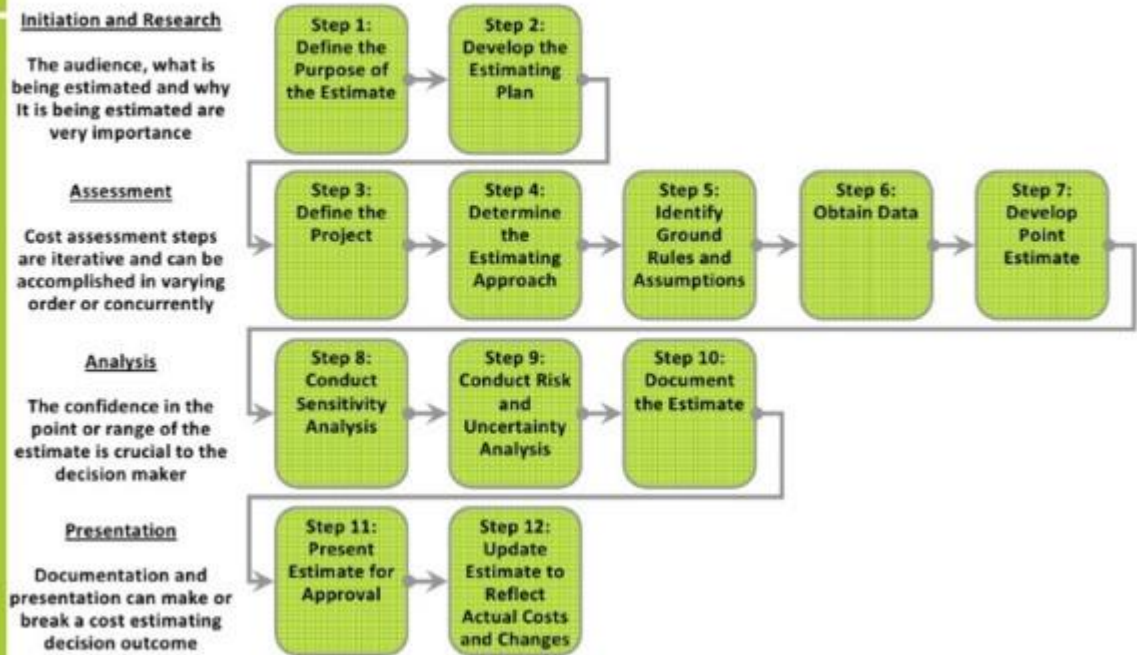
Административные расходы ИТ – обычно включают в себя стоимость косвенных расходов, таких как аренда помещений, канцелярские принадлежности, связь и т.п. Персонала ИТ департамента, чья деятельность не направлена напрямую на сопровождение сервиса. Сюда же могут быть отнесены все расходы, связанные с административной деятельностью ИТ департамента. Обычно являются «постоянным» видом расходов и распределяются пропорционально, по пользователям, сервисам или иным способом.

Прочие «переменные» расходы – можно рассматривать как например, расходы на картриджи для сервиса печати. Эти расходы не учитываются как стоимость ИТ сервиса и переносятся как правило на сторону пользователя.



Необходимо принять во внимание современную тенденцию учета стоимости ИТ сервисов.

Cost Estimating Process



Традиционная модель, используемый во множестве компаний, подразумевает «фиксированный» метод формирования стоимости ИТ сервиса, при котором стоимость сервиса относительно постоянная величина. Например, вы используете почтовый сервис для отправки и приема почты. Вам выделены определённые ресурсы: размер почтового ящика, максимальный объем письма, установлены параметры по доступности сервиса и т.п. Вне зависимости от того, используете вы сервис или нет, вы за него платите.



Вторая модель, формирует стоимость сервиса на основе того, насколько вы его используете. Больше пользуетесь – больше платите. С развитием облачных технологий и появлением инструментов и решений автоматического предоставления и учета используемых ресурсов, данный метод все больше и больше востребован. «Де-факто» основной метод для «облачных» сервисов.

Правильное формирование стоимости ИТ сервиса помогает наиболее точно распределить стоимость между сервисами, что в конечном итоге ведет к эффективности планирования и оценки стоимости и ценности ИТ сервисов.

Расчет стоимости базового сопровождения сервиса

При расчете стоимости сервиса необходимо рассчитать стоимость базовое сопровождение сервиса со стороны ИТ департамента. Базовое сопровождение включает в себя обновление компонентов, мониторинг, проведение регламентных работ, устранение неисправностей и т.п. Для качественного внедрения и сопровождения сервиса необходимы специалисты:

- Уровень эксперта или инженера (L3) – обладающего глубокими знаниями и продолжительным опытом в узкой предметной области. Данный сотрудник необходим для разработки, планирования, внедрения, формирования метрик и поиска неисправностей при некорректном поведении сервиса. Кроме этого он способен на быстрое принятие решения при внештатном поведении сервиса.

- Уровень специалиста (L2) – обладающего базовыми знаниями и некоторым опытом в определённой предметной области. Данный сотрудник необходим для проведения регламентных работ, проведение мониторинга, оказание содействия при внедрении и сопровождении сервиса, разрешения инцидентов и т.п.

- Уровень техника (L1) – обладающего базовыми знаниями и возможно некоторым опытом в определённой предметной области. Данный сотрудник необходим для оказания содействия при внедрении и сопровождении сервиса. В основном используется для выполнения отдельных простых действий. Как правило, используются специалисты подразделения Поддержки Пользователей.

Кроме этого, на основе перечня регламентных работ и важности сервиса, количества компонентов и сложности архитектуры, можно определить количество времени, необходимого для сопровождения сервиса. Для примера, можно использовать следующую таблицу для базового сопровождения сервиса Активного Каталога:

- Уровень инженера (L3) – 15 минут в день на мониторинг (8 часов в месяц).

- Уровень инженера (L2) – 30 минут в день на мониторинг и разрешение инцидентов (16 часов в месяц).
- Уровень инженера (L3) – порядка 5—10 минут в день на поддержку (2.4 часа в месяц).

Стоимость базового сопровождения сервиса департаментом ИТ:

Уровень поддержки базовой	Цена человека-часов USD	Стоимость за 1 месяц		Стоимость за 1 год		Стоимость за 5 лет	
		часов	USD	часов	USD	часов	USD
Infrastructure, L3	15.00	8	120.00	96	1,440.00	480	7,200.00
Infrastructure, L2	10.00	16	160.00	192	1,920.00	960	9,600.00
Help Desk, L1	5.00	4	20.00	48	240.00	240	1,200.00
TOTAL		28	300.00	336	3,600.00	1,680	18,000.00

* - в расчет принимается 12 месяцев, 20 рабочих дней в месяц (пятидневка), 8-ми часовой рабочий день, 160 часов в месяц.

Кроме этого, необходимо отметить, что на количество сотрудников и их уровень в значительной степени влияет соглашения об уровне услуг.

Расчет стоимости поддержки пользователей

При расчете стоимости поддержки пользователей можно использовать два основных показателя: стоимость рабочего времени сотрудников ИТ департамента, в основном это сотрудники подразделения Поддержки Пользователей уровня L1 и специалисты L2/L3, и стоимость систем сопровождения. Расчет зависит от точности ведения учета (например, наличие работающего процесса Управления Инцидентами и т п). Для простоты расчетов и планирования, можно использовать приближенные значения, полученные опытным путем. Так в зависимости от организации на каждые 50 сотрудников необходимо наличие одного специалиста ИТ департамента уровня L1. Из опыта могу сказать, что при правильной организации работы ИТ соотношение может доходить до 150. На количество сотрудников подразделения поддержки пользователей в значительной степени влияет соглашения об уровне услуг.

Упрощенная модель расчета стоимости

Необходимо понимать, что для компаний не оказывающей ИТ услуги и соответственно не приносящей прибыли, основная задача подразделения – снижения расходов. Если нет требований со стороны бизнеса, то желательно тратить как можно меньше ресурсов на административную деятельность подразделения. На начальном этапе, или же при использовании «красной» модели финансирования, возможно вести оценку стоимости ИТ по стоимости расходов. При этом максимально упростив расчеты и использовать приблизительные методы. Приближенные фиксированные расходы за период (обычно год) складываются из следующих составляющих:

Прямые расходы

- Стоимость ИТ активов (Оборудование, программное обеспечение, лицензии и т п)
- Стоимость обслуживания ИТ активов от сторонних компаний (провайдер и т п)
- Стоимость заработной платы сотрудников ИТ департамента, премий и т п. Стоимость может быть распределена по двум возможным методам:
 - пропорционально по количеству обслуживаемых портфелей или организаций
 - пропорционально по количеству сервисов, предоставляемых ИТ департаментом

Косвенные расходы

- Стоимость административных расходов ИТ департамента
- Стоимость дополнительных ИТ компонентов (тестовой площадки, прототипа и т п)
- Стоимость транспортных расходов сотрудников ИТ
- Стоимость инженерных систем
- Стоимость обслуживание инженерных систем

- Коммунальные расходы

Стоимость ИТ активов предполагает учет общих ИТ ресурсов, таких как сервера, коммутаторы, сетевые печатающие устройства и т.п. Стоимость персональных компьютеров сотрудников компании, персональные принтеры не учитываются. Далее, в случае предоставления сервисов разным компаниям, общие расходы на ИТ делятся пропорционально между компаниями по количеству сотрудников. Преимущества: Простота ведения, дает приблизительные расходы на ИТ.

Недостатки: Невозможно оценивать стоимость предоставления по ИТ сервисам.

Полная модель расчета стоимости

При использовании «желтой» или «зеленой» модели финансирования, или по готовности компании, возможно вести оценку стоимости ИТ по стоимости реально предоставляемых сервисов. Расходы на внедрение и сопровождение ИТ рассчитываются также, как и в первом случае, но дополнительно в разрезе ИТ сервиса.

Прямые расходы на ИТ сервис (выделенный или общий) в разрезе на бизнес подразделение или компанию

Постоянные, в процессе внедрения сервиса

- Стоимость ИТ активов (Оборудование, программное обеспечение, лицензии и т.п.) являющихся компонентами данного сервиса
- Стоимость внедрения данного сервиса от сторонних компаний (провайдер и т.п.)
- Стоимость «тестовой» площадки и «прототипа» сервиса
- Стоимость ресурсов по планированию и внедрению
- Стоимость ресурсов по обновлению сервиса

Постоянные, в процессе сопровождения сервиса

- Стоимость ИТ активов (Оборудование, программное обеспечение, лицензии и т.п.) являющихся компонентами данного сервиса
- Стоимость лицензирования на пользователя (если лицензируется на срок использования основных компонентов)
- Стоимость лицензирования на устройство (если лицензируется на срок использования основных компонентов)
- Стоимость обслуживания данного сервиса от сторонних компаний (провайдер и т.п.), если стоимость относительно постоянная

Переменные, в процессе сопровождения сервиса

- Стоимость лицензирования на пользователя (если лицензируется на срок непосредственного использования)
- Стоимость лицензирования на устройство (если лицензируется на срок непосредственного использования)
- Стоимость обслуживания данного сервиса от сторонних компаний (провайдер и т.п.), если предполагается их изменение
- Стоимость заработной платы сотрудников ИТ департамента, премий и т.п. в пересчете на время, затраченное на внедрение и сопровождение сервиса.

Косвенные расходы:

- Стоимость административных расходов ИТ департамента
- Стоимость транспортных расходов сотрудников ИТ

- Стоимость инженерных систем
- Стоимость обслуживания инженерных систем
- Коммунальные расходы (на электричество, вода и т п)

Косвенные расходы можно принять как фиксированные расходы пропорционально разделенные по всем ИТ сервисам.

Преимущества:

- Дает более точную оценку стоимости ИТ
- Возможность реальной оценки использования ИТ ресурсов со стороны компаний
- Возможность вести оценку стоимости на основе ИТ сервисов, предоставляемых компаниям
- Предоставляет возможности финансового планирования и прогнозирования

Недостатки:

- Для внедрения требует высокий уровень организации ИТ
- Большие накладные расходы (дополнительные сотрудники, учетные системы и т п).

Пример расчета стоимости сервиса

Расчет стоимости вычислительных ресурсов (А)

При расчете стоимости сервиса необходимо первоначально рассчитать стоимость активов. Так как наши сервисы предоставляются на платформе виртуализации, то сперва требуется рассчитать стоимость ресурсов:

№	Вычислительные ресурсы	Стоимость, USD	\$	Дополнение
1	C01 платформа виртуализации за 3 года	264,000.00		
1.1	C01 платформа виртуализации	240,000.00		CPU = 380 RAM = 1,900.00 GB VMs quantity = 200
1.2	C01 платформа виртуализации сопровождение 3 года (+10%)	24,000.00		Ремонт, замена и т п
2	C01 платформа виртуализации за 3 года	203,200.00		
2.1	C01 платформа виртуализации	127,00.00		Лицензирование
2.2	C01 платформа виртуализации сопровождение за 3 года	76,200.00		Лицензирование + 60%
3	C02 Система Хранения Данных за 3 года	550,000.00		
3.1	C02 Система Хранения Данных	500,000.00		VM OS = 8,6 TB VM Page File = 2,6TB VM DATA = 31,2 TB
3.2	C02 Система Хранения Данных сопровождение за 3 года (+10%)	50,000.00		Ремонт, замена и т п
4	A05 Система Резервного Копирования за 3 года	176,000.00		
4.1	A05 Система Резервного Копирования	160,000.00		Data Backup = 61 TB
4.2	A05 Резервное Копирование сопровождение за 3 года (+10%)	16,000.00		Ремонт, замена и т п
5	C03 Ядро сети за 3 года	220,000.00		
5.1	C03 Ядро сети	200,000.00		Для 200 Виртуальных Машин
5.2	C03 Ядро сети сопровождение 3 года (10%)	20,000.00		Ремонт, замена и т п

Стоимость компонентов зависимых сервисов

№	Вычислительные ресурсы	Стоимость, \$ USD	Формула и значения
1	C01 платформа виртуализации за 3 года (C1(T))	264,000.00	
1.1	Стоимость логических ядер (CPU(T))	* 132,000.00	CPU = 380
1.2	Стоимость оперативной памяти (RAM(T))	* 132,000.00	RAM = 1,900.00 GB
1.3	Стоимость 1 логического ядра на 3 года (CPU(3))	347.37	CPU(3) = CPU(T) / 380
1.4	Стоимость 1 GB Опер. Памяти на 3 года (RAM(3))	69.47	RAM(3) = RAM(T) / 1900
1.5	Стоимость 1 логического ядра за год (CPU(1))	115.79	CPU(1) = CPU(3) / 3
1.6	Стоимость 1 GB Опер. Памяти за год (RAM(1))	23.16	RAM(1) = RAM(3) / 3
1.7	Стоимость лицензирования за 3 года (OSE(T))	203,200.00	для VM=200
1.8	Лицензирования 1 гостевой системы за 3 года (OSE(3))	** 1,016.00	OSE(3) = OSE(T) / 200
1.9	Лицензирования одной гостевой системы на год (OSE(1))	338.67	OSE(1) = OSE(3) / 3
2	C02 Система Хранения Данных за 3 года (C2(T))	550,000.00	42 TB operation capacity
2.1	Стоимость хранения 1 GB на 3 года (HDD(3))	*** 13.01	HDD(3) = C2(T) / 42,000 GB
2.2	Стоимость хранения 1 GB за год (HDD(1))	4.36	HDD(1) = HDD(3) / 3
3	A05 Система Резервного Копирования (A5(T))	176,000.00	61 TB operation capacity
3.1	Стоимость хранения 1 GB на 3 года (RD(3))	2.88	RD(3) = A5(T) / 61,000 GB
3.2	Стоимость хранения 1 GB за год (RD(1))	0.96	RD(1) = RD(3) / 3
4	C03 Ядро сети за 3 года (C3(T))	220,000.00	
4.1	Использования одной гостевой системы за 3 года (NET(3))	** 1,100.00	NET(3) = C3(T) / 200
4.2	Использования одной гостевой системы на год (NET(1))	366.67	NET(1) = NET(3) / 3

*- Принимаем что стоимость распределена равномерно на процессоры и память.

** - Принимаем что количество возможных развернутых машин порядка 200.

***- Принимаем в расчет суммарную стоимость емкости хранения.

Стоимость единицы компонентов зависимых сервисов

Если есть возможность можно рассчитывать по типам используемых дисков.

Расчет стоимости сервиса (Б)

Пример расчета стоимости сервиса активного каталога (P01) на платформе виртуализации для 100 пользователей принимаем:

№	Вычислительные ресурсы	Значение	Дополнение
1	Компоненты сервиса P01	2	VM XS-size
1.1	Количество логических ядер (CPU(T))	2	2 x 1 CPU
1.2	Количество оперативной памяти (RAM(T))	8 GB	
1.3	Количество лицензированных гостевых систем (OSE(T))	2	
1.4	Емкость хранилища OSE (HDD(T))	80 GB	
1.5	Емкость хранилища резервных копий (RD(T))	960 GB	
1.6	Количество гостевых систем использующих сеть (NET(T))	2	

Требуемые мощности для сервиса P01 (Активного Каталога и DNS)

Расчет стоимости требуемых мощностей для сервиса P01 (Активного Каталога и DNS) на один год

№	Вычислительные ресурсы	Формула	Стоимость, \$ USD
1	Компоненты сервиса P01		
1.1	Количество логических ядер (CPU(T))	2 x \$ 115.79	231.58
1.2	Количество оперативной памяти (RAM(T))	8 x \$ 23.16	185.28
1.3	Количество лицензированных гостевых систем (OSE(T))	2 x \$ 338.67	677.34
1.4	Емкость хранилища OSE (HDD(T))	80 x \$ 4.36	348.80
1.5	Емкость хранилища резервных копий (RD(T))	960 x \$ 0.96	921.60
1.6	Количество гостевых систем использующих сеть (NET(T))	2 x \$ 336.67	673.34
	Полная стоимость вычислительных ресурсов		3,037.94

Для упрощения расчетов можно также использовать стоимость готовых виртуальных машин (например, набор виртуальной машины размера XS-size: 1 CPU, 4GB RAM, 40GB HDD + Windows 2016 Standard OSE),

Фиксированная стоимость ИТ активов (вычислительных ресурсов сервиса) составляет 3,037.94 долларов в год.

Расчет стоимости использования сервиса на пользователя (В)

Расчет стоимости использования сервиса активного каталога (P01) на 100 пользователей принимаем:

№	Вычислительные ресурсы	Формула	Стоимость, \$ USD
1	Стоимость лицензии пользователя (Windows CAL per USER)	100 x \$ 30.00	3,000.00
	Полная стоимость		3,000.00

Расчет стоимости на пользователя для сервиса P01 (Активного Каталога и DNS) на один год

Расчет стоимости базового сопровождения сервиса со стороны ИТ департамента (Г)

Базовое сопровождение сервиса со стороны ИТ департамента включает в себя обновление, устранение неисправностей и т.п. Кроме этого базовое сопровождение сервиса включает в себя 360 часов поддержки пользователей.

Уровень базовой поддержки	Цена человека-часов USD	Стоимость за 1 месяц		Стоимость за 1 год		Стоимость за 5 лет	
		часов	USD	часов	USD	часов	USD
Infrastructure, L3	15.00	5	75.00	60	900.00	300	4,500.00
Infrastructure, L2	10.00	5	50.00	60	300.00	300	3,000.00
Help Desk, L1	5.00	20	100.00	240	1,200.00	1,200	6,000.00
TOTAL		30	225.00	360	2,400.00	1,800	13,500.00

* - в расчет принимается 12 месяцев, 20 рабочих дней в месяц (пятидневка), 8-ми часовой рабочий день.

Стоимость базового сопровождения сервиса департаментом ИТ:

Расчет стоимости административных издержек по сопровождению сервиса (Д)

Стоимость сопровождения (обслуживания ИТ активов) сервиса

Стоимость сопровождения (обслуживания ИТ активов) сервиса со стороны сторонних компаний равна нулю.

Стоимость технических сервисов, обеспечивающих внедрение и сопровождение сервиса (сервер обновлений, тестовая площадка и т.п.). Может рассчитываться как отдельный сервис, так и как усредненное значение. Принимая мощность тестовой площадки из соотношения 25% и прочие расходы.

Стоимость, которая некоторых составляющих может быть рассчитана другими вариантами:

Стоимость заработной платы сотрудников ИТ департамента

Стоимость заработной платы сотрудников ИТ департамента может быть распределена:

пропорционально по количеству обслуживаемых портфелей или организаций

пропорционально по количеству сервисов, предоставляемых ИТ департаментом

из расчета времени, затраченного на обслуживание и сопровождение сервисов

Принимаем для расчета усредненную стоимость пропорционально количеству сервисов, предоставляемых ИТ департаментом. Принимаем годовые расходы на ИТ департамент 150,000.00 долларов в год и количество сервисов 50. Тем самым получаем 3,000.00 долларов за сервис в год.

Стоимость расчета косвенных расходов сотрудников ИТ департамента

Стоимость косвенных расходов также может быть распределена следующими методами:

- пропорционально по количеству обслуживаемых портфелей или организаций
- пропорционально по количеству сервисов, предоставляемых ИТ департаментом
- из расчета реальных затрат на обслуживание и сопровождение сервисов

№	Вычислительные ресурсы	Стоимость, \$ USD
1.1	Стоимость ИТ активов	3,037.94
1.2	Стоимость пользовательских лицензий на 100 пользователей	3,000.00
2	Стоимость обслуживания ИТ активов со стороны третьей стороны	0.00
3	Стоимость базового сопровождения со стороны ИТ департамента	2,400.00
	Прямые расходы	8,437.94
4	Административные расходы ИТ департамента	1,000.00
5	Стоимость сопровождения инженерных систем	200.00
6	Стоимость потребления электричества	200.00
	Косвенные расходы	1,400.00
	Полная стоимость вычислительных ресурсов	10,837.94

Полная стоимость для сервиса P01 (Активного Каталога и DNS) на один год

Расчета стоимости рабочего места

Расчет стоимости рабочего места сотрудника позволяет планировать бюджет при расширении бизнеса, оценки эффективности работы сотрудника, департамента, себестоимость продукта и т.п. В качестве параметров для формирования стоимости можно взять следующие значения:

- Стоимость компьютера
- Стоимость операционной системы и программного обеспечения, установленного на компьютере
- Стоимость офисного оборудования (принтеры, копиры)
- Стоимость сервисов, используемых пользователем
- Стоимость расходов пропорциональна распределённая между пользователями
- Стоимость клиентского доступа к сервисам

№	Продукты и решения	PRICE \$	Дополнение
1	Стоимость персонального компьютера	1,500.00	Разовая оплата
2	Стоимость операционной системы Windows компьютера	194.00	Разовая оплата
3	Стоимость обновления (SA) операционной системы компьютера	75.00	Enterprise Agreement SA
4	Стоимость пакета офисных приложений Microsoft Office 2016 Pro	228.00	
5	Стоимость программы Microsoft Project 2016 Pro	582.00	Include Project CAL
6	Стоимость программы архивирования	20.00	
7	Стоимость персональной защиты (Anti-virus, Firewall, Device Control)	100.00	

№	Лицензии клиентского доступа (CAL)	PER DEVICE	PER USER	Продукты и сервисы
	Пакет доступов Enterprise CAL Suite (Доступ к «Enterprise» продуктам: Windows, Exchange, Skype, SharePoint, SCCM)	235.00		P01, P02, P03, P04, S01, S02, S03, S05, S06, S07, S08, A01, A03, A04, A09, D03, D04, D14, D15,
	Пакет доступов Core CAL Suite (Доступ к «Standard» продуктам: Windows, Exchange, Skype, SharePoint, SCCM)	120.00		P01, P02, P03, P04, S01, S02, S03, S05, S06, S07, S08, A01, A03, A04, A09, D03, D04, D14, D15,
	Доступ к Windows серверам (Windows CAL)			P01, P02, P03, P04, S01, S02, S03, S05, S06, S07, S08, A01, A03, A04, A09, D03, D04, D14, D15,
	Доступ к Exchange серверам (Exchange CAL)			S06,
	Доступ к Skype for Business серверам (Skype CAL)			S07,
	Доступ к SharePoint серверам (SharePoint CAL)			S08,
	Доступ к компонентам System Center 2016			
	Доступ к Project серверам (Project CAL)	127.00		S09,
	Доступ к SCCM серверам (SCCM CML CAL)			A04,
	Доступ к SQL серверам (SQL CAL)	122.00	122.00	P04, S07, S08, D14,
	Доступ к Identity Management серверам (MIM CAL)	11.00		D13,

* Цены могут различаться в зависимости от выбранной модели лицензирования и т.п.

Результативность и эффективность ИТ

Расчет эффективности ИТ департамента позволяет оценить эффективность работы ИТ департамента, позволяет планировать бюджет при расширении бизнеса, оценки эффективности работы сотрудника, департамента, себестоимость продукта и т.п.

В качестве параметров для расчета эффективности ИТ департамента можно принять, но не ограничиваться:

- Стоимость ИТ активов, используемых в организации
- Стоимость ИТ департамента (заплата, премии, обучение и т.п.)
- Стоимость ИТ услуг оказываемых третьей стороной, по сопровождению ИТ активов
- Стоимость бизнес сервисов, сопровождаемых ИТ департаментом
- Стоимость технических сервисов, сопровождаемых ИТ департаментом

Помимо определённых выше метрик, для повышения точности и эффективности оценки стоимости ИТ, могут использоваться следующие показатели:

- Стоимость ИТ оборудования
- Стоимость лицензий
- Стоимость систем резервного хранения и архивирования
- Стоимость сопровождения со стороны третьих лиц
- Стоимость сопровождения со стороны ИТ департамента
- Стоимость «тестовой» площадки и «прототипа» сервиса
- Процент соотношения ИТ оборудования к полной стоимости ИТ активов
- Средний срок (стоимость) использования ИТ активов
- Средняя стоимость решения инцидента
- Средняя стоимость решения проблемы

Кроме этого желательно принимать во внимание следующие факторы:

- Не использованные возможности – например, ваши пользователи используют только активный каталог и файловый сервис (Windows CAL). Но закуплены лицензии на пользователя (Core CAL Suite). Возможности второго варианта шире (дополнительно доступ к продуктам Exchange, SharePoint, System Center Configuration Manager Client ML), но и стоимость также выше. Тем самым стоимость решения для портфеля обходится выше, чем возможно.

- Стоимость компонентов платформы, являющейся не отделимой составляющей сервиса. Например, стоимость серверной операционной системы сервера для обмена файлами (файловый сервер) является «нулевой», но при этом она учтена в процессе лицензирования платформы виртуализации. В этом случае все стоимость определяется для каждого сервиса на основе фиксированной распределенной стоимости. Т. е. как механизм расчета можно взять возможности платформы виртуализации по максимальному количеству гостевых серверов к стоимости лицензирования.

Кроме прямых финансовых показателей взглянем на эффективность ИТ с другого ракурса. Предположим, что перед ИТ ставится следующая задача:

Для ведения бизнеса организации требуется определённая информационная система «С» (назовем ее для примера ERP). Кроме этого для ведения бизнеса необходима вспомогательная система «В», например, сервер почтовых сообщений, позволяющая вести переписку с клиентами. Руководство компании считает, что система «С» крайне важна и ее простой несет убытки для бизнеса, в то время незначительный простой второй системы «В» не влияет на ведение бизнеса. ИТ департамент также знает, что для развертывания данных бизнес систем, необходимо развернуть технический сервис «А», например, Сервис Активного Каталога, без которого работа бизнес систем невозможна. Как видно из диаграммы ниже, взгляды бизнеса и ИТ могут не совпадать. Бизнес видит, что ему критически важна система «С» и важна система «В», в то время он ничего не знает про систему «А». ИТ не разбирается в важности бизнес систем, но знает, что без технического сервиса «А» запуск двух других не возможен. В итоге, бизнес и ИТ нашли общий язык и результат: критически важные системы «А» и «С» и важная система «В». Бизнес выделил финансы и ИТ приступил к планированию ИТ инфраструктуры. В нашем примере, предположим, что все три системы требуют одинаковые вычислительные ресурсы. Рассмотрим варианты реализации.

Классический пример Вариант 1: Закупается три одинаковых физических сервера (PH1, PH2 и PH3). На каждый устанавливается необходимая система «А», «В» и «С» соответственно. Показатели серверов:

P – Производительность (Performance), хорошие, условно примем 2 из 3.

C – Стоимость (Cost), не дешевые (тоже 2 из 3). Сервера известных производителей с хорошими показателями. Примем стоимость серверов как 2,000 условных единиц каждый.

U – Загруженность (Utilization) – сервера загружены лишь на треть (1 из 3).

Кроме этого требуется обеспечить возможность восстановления данных в случае ошибок, сбоев или активности вирусов. Для этого ИТ департамент купил недорогое решение для резервного копирования данных на внешние носитель (внешний жесткий диск). В общей сложности три диска, каждый из которых стоит по 100 условных единиц. Параметры системы резервного копирования: скорость копирования/восстановления – средняя. И в дополнение решения, необходимо обеспечить каждый сервер Источником Бесперебойного Питания (ИБП) по 200 условных единиц каждый, которые обеспечивают некоторое время работу серверов

и позволят безопасно выключить их при долговременном отключении электричества. ИБП отнесем к системам обеспечения. В итоге получает следующую таблицу для анализа:

№	Сервис	Важность сервиса	Тип Сервиса	Стоимость	Описание
1	«А»	Критичный	Технический	2,000	Возможности сервера хорошие (2), использование сервера низкое (1), имеется потенциал роста.
2	«В»	Важный	Бизнес	2,000	
3	«С»	Критичный	Бизнес	2,000	
4	Бэкап	Важный	Технический	3 x 100	Скорость восстановления средняя
5	ИБП	Важный	Обеспечение	3 x 200	Время работы низкое

Результаты решения Варианта 1:

Полная стоимость решения – 6,900 из которой

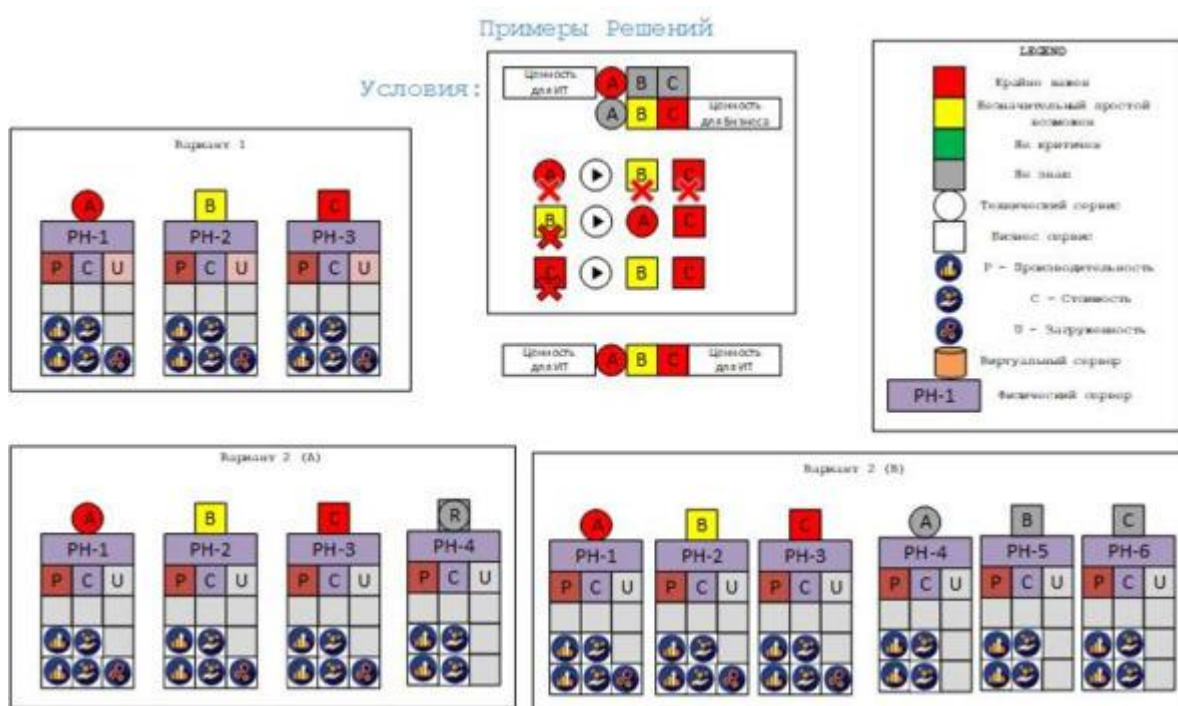
- стоимость бизнес сервисов 58%,
- технических сервисов – 32%
- обеспечения – 9%.
- Стоимость бизнес сервисов «А» и «В» – 87% от полной стоимости расходов на сервис (2,000 +100 +200 на каждый сервис).

Время восстановления данные удовлетворительна для сервиса «В», но не удовлетворительна для «А» и «С».

ИБП обеспечивает защиту бизнеса от кратковременных перебоев электропитания,

Доступность сервисов при отказе оборудования – отсутствует, сервис восстановит работу после ремонта. При этом при отказе сервиса «А» остановится работа бизнеса.

Для того, чтобы обеспечить доступность сервисов при сбое оборудования, ИТ департамент предложил решение Вариант 2 (А), в котором добавляется один резервный сервер. При поломке одного из серверов, сервис восстанавливается на резервном физическом сервере, пока основной сервер в ремонте. Недостаток в том, что при отказе двух серверов одновременно, бизнес так же останавливается.



Чтобы обеспечить 100% доступность сервисов необходимо, продублировать все сервера плюс иметь в резерве как минимум один дополнительный ИБП и диск для резервного копирования. Это обеспечивается решением Вариант 2 (В):

№	Сервис	Важность сервиса	Тип Сервиса	Стоимость	Описание
1	«А»	Критичные	Технический	2,000	Возможности сервера хорошие (2), использование сервера низкое (1), имеется потенциал роста.
2	«В»	Важный	Бизнес	2,000	
3	«С»	Критичные	Бизнес	2,000	
4	Бэкап	Важный	Технический	4 x 100	Один дополнительный носитель для резервного копирования
5	ИБП	Важный	Обеспечение	4 x 200	Один дополнительный ИБП
6	Резерв	Важный	доступность	3 x 2,000	Защита от поломки всех серверов

Результаты решения Варианта 2 (В):

Полная стоимость решения – 13,200 из которой

- стоимость бизнес сервисов 30%,
- резервного оборудования – 48%,
- технических сервисов – 17%
- обеспечения – 5%.
- Стоимость бизнес сервисов «А» и «В» – 45% от полной стоимости расходов на сервис (2,000 +2,000 +100 +200 + (300/3)).

Время восстановления данные удовлетворительна для сервиса «В», но не удовлетворительна для «А» и «С».

ИБП обеспечивает защиту бизнеса от кратковременных перебоев электропитания,

Доступность и резервирование сервисов при отказе оборудования – полная, обеспечивается защита всех серверов сервисов. А также имеется частичное, один к трем, аппаратное резервирование ИБП и средств резервного копирования.

Для обеспечения указанных характеристик, стоимость решения выросла почти в два раза (на 91%). Далее, для обеспечения аварийного электропитания, необходимо будет приобрести генератор и т.п.

№	Сервис	Важность сервиса	Тип Сервиса	Стоимость	Описание
1	«А», «В», «С»	Критичные	Технический	2,000	Все сервисы на одном физическом сервере, Возможности сервера хорошие (2), использование сервера высокое (3),
2	Бэкап	Важный	Технический	3 x 100	+1 резервный
3	ИБП	Важный	Обеспечение	3 x 200	+1 резервный
4	Резерв	Важный	Доступность	2,000	Защита от поломки всех серверов
5	Виртуализация	Критичные	Технический	1,000	

Теперь рассмотрим еще одно решение *Вариант 3:*

В данном решении используется технология виртуализации, которая позволяет запускать на одном физическом сервере несколько виртуальных серверов. Как видим из диаграммы, те же физические сервера можно использовать на полную мощность при той же стоимости.

Результаты решения Варианта 3:

Полная стоимость решения – 5,900 из которой

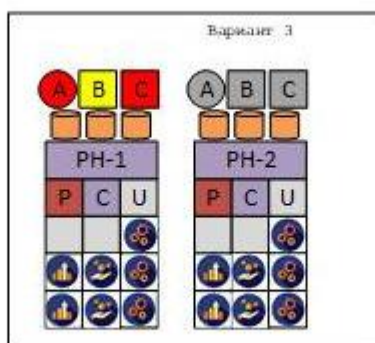
- стоимость бизнес сервисов 33%,

- резервного оборудования – 33%,
- технических сервисов – 30%
- обеспечения – 4%.
- Стоимость бизнес сервисов «А» и «В» – 45% от полной стоимости расходов на сервис (2,000 +2,000 +100 +200 + (300/3)).

Время восстановления данных удовлетворительна для сервиса «В», но не удовлетворительна для «А» и «С».

ИБП обеспечивает защиту бизнеса от кратковременных перебоев электропитания,

Доступность и резервирование сервисов при отказе оборудования – полная, обеспечивается защита всех серверов сервисов. А также имеется частичное, один к двум, аппаратное резервирование ИБП и средств резервного копирования.



Сравнивая решения Вариант 3 более правильное, обеспечивает те же возможности, что и Вариант 2 (В) и даже лучше, при стоимости решения дешевле более чем в два раза.

Вторая сторона вопроса, сотрудники ИТ, которые разрабатывают, внедряют и сопровождают ИТ сервисы. Стоимость сотрудника ИТ колеблется от 6,000 условных единиц до десятков тысяч в год, в зависимости от компетенции. Для небольших компаний содержание выделенного штата ИТ может быть не целесообразно. Как вариант, часто используется схема, когда в штате имеется сотрудник – который выполняет функции куратора ИТ вопросов. Все вопросы по поддержке пользователей и внедрении решений переданы на аутсорсинг.

Для более-менее серьезной организации, наличие собственного штата ИТ позволяет устранить недостатки аутсорсинга, снизить издержки, поддержать связь между бизнесом и ИТ с накоплением знаний. При этом, некоторые задачи могут оставаться на аутсорсинге (например, внедрение ИТ решений которые требуют детальной проработки со стороны экспертов различных направлений ИТ, людские ресурсы при внедрении, сопровождение специфических информационных систем и т п), в то время как сопровождение «общих» ИТ решений может оставаться за локальным ИТ, так как менее требовательно к ресурсам и компетенции.

Подводя итоги можно понять, что грамотное планирование архитектуры решения может повысить эффективность ИТ. Задачи ИТ – обеспечить выполнение требований бизнеса и снизить стоимость технических сервисов, обеспечить правильный баланс ресурсов между бизнес сервисами и техническими сервисами, обеспечивающими их функционирование. Оценка ИТ департамента должна включать в себя оценку ИТ решений, внедренных в организации, архитектуру и организацию деятельности.

В современном мире имеются готовые показатели ИТ затрат с сегментированием по отраслям или направлениям деятельности. Так для примера:

- Показатели затрат на ИТ как доля с оборота (порядка 1—4%),
- Доля ИТ затрат на одного сотрудника (1000—5000 долларов),
- Показатели ИТ затрат для классического банка – порядка 10—15%,

- Показатели ИТ затрат для розничного банка или банка микрофинансирования – 15—25%.
- Стоимость затрат на ИТ персонал порядка 10—15% от стоимости активов.
- Стоимость технических сервисов не более 30% от стоимости ИТ инфраструктуры.

Заключение

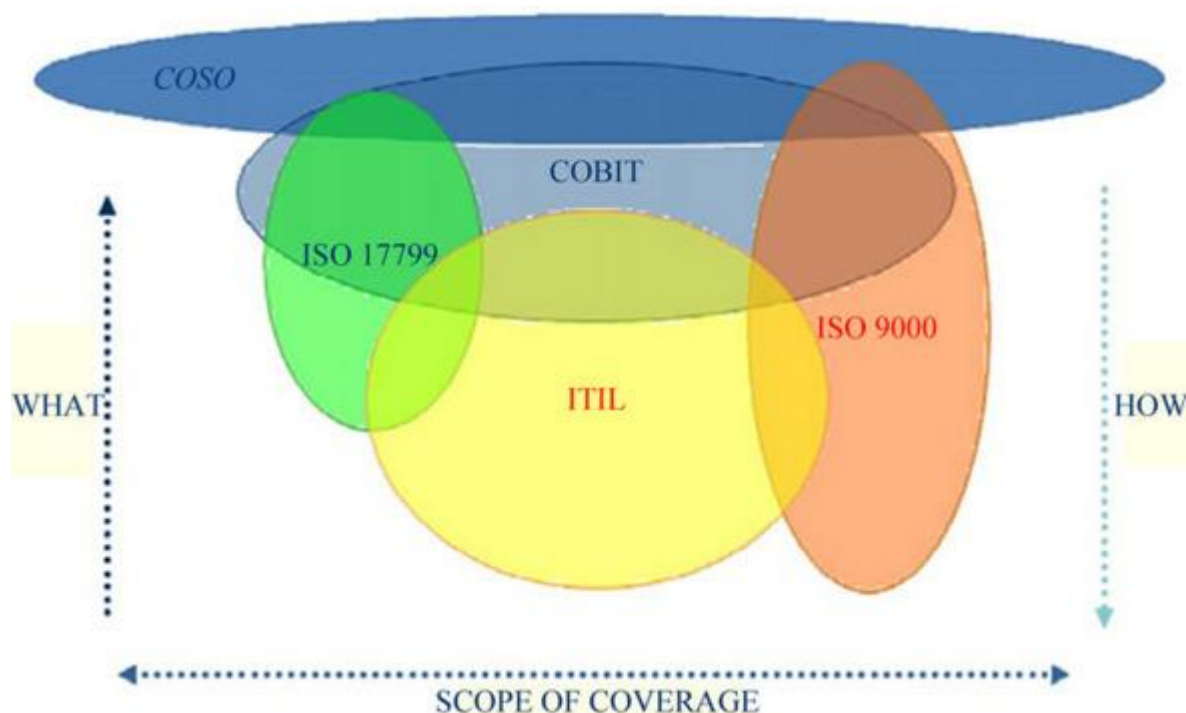
Для эффективного управления финансами в ИТ департаменте, рекомендуется внедрить следующие элементы:

- Введите учет рабочего времени сотрудников
- Введите дисциплину распределять рабочее время по проектам, задачам.
- Определите стоимость часа каждого программиста: для ориентира можно взять текущую зарплату сотрудника и данные о заработке аналогичных специалистов по рынку.
- Старайтесь эффективно распределять трудозатраты по проектам: на проект с небольшим бюджетом посадить сотрудника с невысокой стоимостью часа, чтобы заказ не выполнял тот специалист, который обходится работодателю дороже.
- Рассчитывайте себестоимость услуг и полную стоимость разработки: для этого учитывайте все расходы и сопутствующие траты отдельно по каждому проекту.

Организация Деятельности ИТ

Общие Положения

Организация управления ИТ, корпоративное управление ИТ, рассматривается различными стандартами и лучшими практиками, такими как ISO 20000, ISO 27000, ISO 38500, ISO 31000, ISO 9000, ITIL, а также смежные направления, такие как BASEL II, PMBOK, CMMI, TOGAF, PRINCE2, PCI DSS. Все они описывают деятельность ИТ по уровню детализации, фокусируются на различных аспектах деятельности и областях применения, отвечают на вопросы что делать, как делать и т.п. Многие вопросы и подходы уже рассмотрены в книге более или менее детально.



В данном разделе мы рассмотрим организацию с точки зрения управления ИТ департаментом, сфокусировав внимание на вопросах управления сотрудниками. Основная задача руководителя – это управление сотрудниками на всех этапах функционирования организации, начиная с подбора персонала и до момента, когда сотрудник покидает компанию.

Люди являются основным источником формирования добавленной стоимости и успешности практически любой компании. У двух одинаковых организаций, работающих в одной сфере,

может быть одинаковое оборудование, программное обеспечение, одинаковая организационная структура и другие ресурсы, но различный состав коллектива и атмосфера в организации, что в конечном итоге приведет к росту одной компании и упадку другой.

Структура ИТ департамента

В разделе рассматривается организация управления ИТ. На начальном этапе или малых размеров компании, ИТ может представлять из себя ИТ службу, входящую в состав административного или иного департамента. Далее с ростом компании, ИТ должно быть выделено в отдельный отдел (куратор административного или иного департамента). Следующий этап развития – ИТ может трансформироваться в ИТ департамент и руководитель департамента выходит на «С Level». Дальнейшее развитие ИТ вводятся понятия СІО (Chief Information Officer) и СТО (Chief Technology Officer) и вывод их из состава ИТ департамента и перевод на уровень управления организацией, холдинга. На этом этапе СІО и СТО, как и СІСО (Chief Information Security Officer) представляют интересы не отдельного департамента, а холдинга в целом. Представление ИТ на данном уровне наиболее тесно интегрирует ИТ и бизнес. Дальнейшая трансформация ИТ или бизнеса в состав холдинга вводит новые организационные единицы ИТ:

- ИТ департамент холдинга
- ИТ департамент портфеля
- ИТ департамент компании
- ИТ службы

При организации ИТ необходимо принять во внимание следующий перечень вопросов:

Организационные – Сфера деятельности организации, Миссия и видение компании, Стадии организации (начало бизнеса, работающая организация и т п), Структура организации, Количество сотрудников, Стоимость бизнеса, Ожидания бизнеса от ИТ, Оперативные планы организации, Стратегические планы организации и т п

Технические – Сеть организации (филиалы, объекты и т п), ИТ инфраструктура, Информационные Системы и т п

Технологические – Текущие технология и решения, используемые в ИТ, перспективные решения и т п

Далее могут быть выделены следующие возможные модели управления:

Полностью автономные ИТ департаменты

Полностью автономные ИТ департаменты и службы со слабо выраженной связью с центральным ИТ холдинга или консалтинговой компанией.

Организация взаимодействия:

- Рекомендационные функции
- Центральный ИТ департамент формирует общие принципы ИТ архитектуры
- Центральный ИТ департамент формирует общие ИТ политики
- Собирает информацию по портфелям связанную с функционированием ИТ

Достоинства:

- Низкая стоимость владения
- Быстрое внедрение
- Быстрая реакция ИТ на бизнес требования

Недостатки:

- Контроль и функционирование ИТ инфраструктуры зависит от локального ИТ

- Слабая или отсутствующая связь между целями холдинга и ИТ стратегией компаний
- Не управляемый ИТ бюджет холдинга
- Не управляемая ИТ стратегия холдинга

Централизованный ИТ департамент с сильно связанными функциональными связями

Централизованный ИТ департамент и ИТ департаменты портфелей и компаний, с сильно связанными функциональными связями. ИТ портфелей в достаточной степени самостоятельны и самодостаточные.

Организация взаимодействия:

- Регуляторные функции центрального ИТ холдинга (контроль, требования)
- Центральный ИТ департамент формирует общие принципы ИТ архитектуры и контролирует их исполнение
- Центральный ИТ департамент формирует общие ИТ политики и контролирует их исполнение
- Контролирует активность компаний, связанных с функционированием ИТ
- Предоставление общих сервисов
- Оказание услуг по проектированию, внедрению и сопровождению ИТ сервисов в компаниях, не имеющих достаточной компетенции или ресурсов.

Достоинства:

- Централизованное управление ИТ
- Контроль соответствия ИТ архитектуре холдинга
- Прочная связь между целями холдинга и ИТ стратегией компаний
- Снижение расходов на функционирование ИТ
- Управляемая ИТ стратегия и бюджет
- Повышение Информационной Безопасности
- Быстрая реакция ИТ на бизнес требования

Недостатки:

- Процесс внедрения зависит от управляемости и степени централизации департаментов холдинга и компаний
- Удлинение цепочки принятия решения

Единый ИТ департамент

Единый ИТ департамент для всего холдинга или организации

Организация взаимодействия:

- Все ИТ службы компаний входят в состав центрального департамента ИТ
- Функционирование ИТ холдинга и компаний централизованное
- На местах остаются лишь подразделения «поддержки пользователей» и ИТ менеджеры

Достоинства:

- Централизованное управление ИТ
- Единая ИТ архитектуре холдинга
- Прочная связь между целями холдинга и ИТ стратегией холдинга и компаний

- Снижение расходов на функционирование ИТ за счет эффекта масштаба, сокращения административных расходов, консолидации ИТ активов и т.п.
- Единая ИТ стратегия и бюджет
- Высокий уровень Информационной Безопасности

Недостатки:

- Процесс внедрения полностью зависит от управляемости и централизации большинства департаментов холдинга и компаний
- Сложный процесс трансформации, уже имеющихся ИТ департаментов компаний, с высоким риском снижения качества обслуживания

Структура ИТ департамента рассматриваемая в примере представляет собой следующие роли и подразделения:

Роль: «IT DIRECTOR» («C Level») – руководит департаментом.

Роль: «IT ARCHITECT» – Формирование ИТ стратегии.

Роль: «IT PROJECT MANAGER» – руководит всеми проектами, связанными с ИТ.

Отдел: «SERVICE DESK» – организационная единица ИТ департамента, обеспечивающий поддержку пользователей уровня L0 и L1. Она может представлять из себя как централизованную, так и локальную структуру. На начальном этапе функционирует как «реактивная» составляющая: «проблема – решение». Далее с развитием подразделения (рост уровня специалистов, организации работ, контроля) принимает «аналитическую» форму – предотвращение инцидентов. Различают следующие возможные структуры Сервис Деска:

- Централизованный центр Поддержки Пользователей (Centralized Service Desk)
- Локальный центр Поддержки Пользователей (Local Service Desk)
- Виртуальный центр Поддержки Пользователей (Virtual Service Desk)

Отдел: «IT INFRASTRUCTURE» – организационная единица ИТ департамента, обеспечивающий полный жизненный цикл ключевых ИТ сервисов, поддержку пользователей уровня L2 и L3. Отдел может включать в себя подразделения и группы. Задачи отдела в сопровождении всех инфраструктурных сервисов, таких как «CORE», «PRIMARY», «SECONDARY» и «DEFENSE».

Отдел: «SOFTWARE DEVELOPMENT» – организационная единица ИТ департамента, обеспечивающий разработку, внедрение, сопровождение и интеграции программных решений, а также поддержку пользователей уровня L2 и L3. Отдел может включать в себя подразделения и группы. Задачи отдела в сопровождении таких сервисов, как «BUSINESS APPLICATIONS» и «INTEGRATION».

Отдел: «IT Security» – организационная единица ИТ департамента (опциональная), обеспечивающий при взаимодействии с департаментом Безопасности разработку, самостоятельное внедрение и сопровождение решений в области Информационной Безопасности. Также обеспечивает поддержку пользователей уровня L2 и L3. Отдел может включать в себя функциональные подразделения и группы. Имеет смысл формирование обособленного отдела в составе ИТ департамента если имеется значительное количество специализированных решений в области информационной безопасности. При незначительном количестве, данные задачи может выполнять отдел «Инфраструктуры».

Также имеются следующие группы и комитеты, имеющие непосредственно отношение к работе ИТ департамента:

ИТ комитет (IT Steering Committee) – Принимает решения по ключевым вопросам функционирования ИТ (ИТ стратегия, бюджет, операционное планирование, план восстановления и непрерывности бизнеса и т.п.). Также выполняет контрольные функции над их исполнением. Основные направления:

- Обзор стратегических ИТ планов и их соответствие бизнес стратегии организации
- Обзор планов и проектов бизнеса и ИТ
- Планирование требований
- Выставление приоритетов по ИТ проектам
- Оценка потенциала по аутсорсингу
- Непрерывность бизнеса и ИТ сервисов
- ИТ Политики и процедуры

Группа реагирования при чрезвычайных ситуациях (Emergency IT team) – Группа специалистов, принимают решения и исполняют их в случае чрезвычайных происшествий.

Комитет по управлению изменениями (Change Advisory Board CAB) – Принимает решения по внесению изменений, определения приоритетов и функционирования ИТ сервисов и контролирует их исполнение.

Комитет по управлению экстренными изменениями (Emergency Change Advisory Board ECAB) – Принимает решения по внесению экстренных изменений.

Комитет по управлению рисками (IT Risk Management Committee) – Разрабатывает, анализирует риски и формирует соответствующие рекомендации, связанные с функционированием ИТ, и следит за их исполнением.

Проектная группа (Project Management Group) – Разрабатывает, планирует и внедряет проекты, связанные с функционированием ИТ, и следит за их исполнением.

Экспертная группа (SME Subject Matter Experts) – Детальная проработка продуктов или процессов и предоставление на ИТ комитете для принятия решения. В состав группы должны входить профильные специалисты бизнеса и ИТ. В отличие от проектной группы, не имеет полномочий по принятию решения, а носит лишь рекомендательную функцию.

Количество и задачи подразделений могут отличаться в зависимости от требований компании. В качестве базового критерия можно принять следующие рекомендации:

- Один руководитель непосредственно может эффективно управлять порядка семью работниками
- Важность или законченность функции в составе подразделения
- Стратегия организации
- Количество и спектр предоставляемых ИТ сервисов
- Цели, задачи и организация ИТ департамента определяются в руководящих документах ИТ.

Управление сотрудниками и контроль взаимоотношений между сотрудниками

Основной ресурс любой компании – это люди. Именно их знания, умения и компетенции приносят деньги. Но это и основная статья затрат. Поэтому от того, как компания управляет этим ресурсом, и зависит ее результативность. Так как именно они формируют продукты и добавленную стоимость. Эффективное управление сотрудниками и контроль взаимоотношений между ними является ключевым фактором успеха. Руководитель несет персональную ответственность за поддержание необходимого микроклимата в рабочей группе.

Поддержание сплоченности рабочей группы – это искусство и наука. Следующие факторы позволяют сплотить сотрудников:

- Необходимое взаимодействие. Чем более сплоченной является группа, тем больше сотрудники будут стремиться стать ее членами, и тем более вероятным будет их следование принятым нормам поведения.
- Общие взгляды и цели. Чем больше сходства во взглядах членов рабочей группы, тем выше вероятность ее сплоченности.

•Подчиненная цель. Сплоченность группы повышается, если существует цель которую ее члены поддерживают.

•Общий «враг». Признание существования общего врага позволяет повысить сплоченность группы.

У•спех в достижении целей. Сплоченность группы растет пропорционально ее статусу.

Препятствия, мешающие эффективному общению, часто можно преодолеть, если их знать. Следующие препятствия на пути установления обратной связи можно преодолеть, если постоянно держать их в поле зрения:

Осуждение

Критика

Оскорбление

Указание недостатков

Высказывание собственных оценок

Силовое решение проблем

Приказание

Угрозы

Поучение

Чрезмерное расспрашивание

Уклонение от решения проблем

Отвлечение внимания

Логический спор

Успокаивание

Эти факторы не нуждаются в разъяснении. Для нахождения общего языка с сотрудниками, необходимо постоянно о них помнить и предпринимать усилия по их преодолению. Для нахождения общего языка с сотрудниками большое значение имеет установление обратной связи. Ниже перечислены рекомендации, которыми предлагается руководствоваться в работе. Обратная связь позволяет сотрудникам взглянуть на себя со стороны.

Провести анализ своих собственных мотивов. Убедиться, что ваша цель – оказать помощь другим, а не показать, насколько вы восприимчивы и хороши, и не обижать других.

Определить, готовы ли сотрудники к установлению обратной связи. Вообще говоря, обратная связь наиболее эффективна, когда ее добиваются, а не навязывают.

Установить обратную связь немедленно, если сотрудники изъявили желание и готовы к ней.

Описать действия сотрудника и ваше мнение о его работе, но не наклеивать ярлыки и оценивать их поступки.

Описывать конкретные события, а не заниматься общими рассуждениями.

Предлагать обратную связь, а не навязывать ее. Предоставлять информацию, которую сотрудник сможет использовать в своей работе, а не командовать.

Предлагать обратную связь как нечто временное. Догматический подход обычно вызывает у людей отрицательную реакцию.

Быть готовым к выслушиванию критики в свой адрес.

Не перегружать сотрудников информацией. Сосредоточить внимание на самом важном и на том, что можно изменить.

Следить за поведением сотрудника при получении информации от него.

Другой стороной сплоченности коллектива является конфликт. Каждый руководитель должен знать способы разрешения конфликтов. Ниже предлагается стратегия решения проблем и разрешения конфликтных ситуаций, которая позволяет обойти подводные камни. Существуют шесть классических этапов совместного разрешения конфликтов:

•Определить проблему с точки зрения требований, а не решений.

•Рассмотреть возможные решения.

•Выбрать решения, которые удовлетворяют требованиям обеих конфликтующих сторон.

•Составить план действий (кто что делает и к какому сроку).

•Реализовать план.

- Оценить, насколько хорошим является выбранное решение.

Требования и критерии отбора сотрудников

Определяет требования к персональным и техническим навыкам сотрудников ИТ департамента для соответствия занимаемой позиции. Правильно выстроенная система позволяет поддерживать высокий уровень качества предоставления ИТ сервисов. Ключевые аспекты включают в себя, но не ограничиваются ниже перечисленными:

Определение требований к руководителю

Руководитель – это один из самых важных сотрудников в ИТ департаменте. Этот человек играет главную роль в организации и контроле за исполнением всех обязанностей ИТ. Руководитель также является «лицом» ИТ департамента в своей организации и для внешних групп. Время, затрачиваемое на выбор ИТ руководителя, может быть разным.

Критерии отбора

Главная цель при выборе руководителя ИТ – назначить на эту должность человека опытного, компетентного и способного получить конечный результат при соблюдении требований. С этой точки зрения все основные качества эффективно работающего руководителя ИТ можно отнести к одной из следующих пяти категорий:

- Образование и опыт
- Лидерство и стратегическое мышление
- Техническая компетентность
- Умение работать с людьми
- Доказанные способности к управлению

Ряд хороших характеристик только по какой-либо одной категории не может быть достаточным основанием для найма на должность руководителя. Перечисленные здесь категории обеспечивают сбалансированный набор основных характеристик для оценки кандидата.

Образование и опыт

Образование и опыт будущего руководителя проекта должна соответствовать характеру и специфике организации. Как говорится, «капля опыта может перевесить тонну теории». Итак, цель – назначить руководителем того, кто может выполнить работу в рамках выделенных средств. Руководитель должен иметь хорошее базовое образование в дополнение к опыту работы в данной области. На практике вы должны искать кандидата, который показывает приемлемое сочетание фундаментальных знаний, аналитического мышления, теории управления и опыта практической работы.

Лидерство и стратегическое мышление

Руководитель ИТ – это лидер, который помогает разрабатывать, координировать, контролировать и выполнять работ ИТ департамента. Руководящая роль и стратегическое мышление означают способность представлять себе и реально воплощать «общую картину», и в то же время, когда идет работа над отдельными задачами. Это означает способность видеть лес за деревьями. Стратегическое мышление также предполагает способность формулировать «наводящие вопросы», которые контролируют промежуточные цели и запланированный конечный результат. Руководитель должен уметь отделить стратегические размышления, планирование и решения от тактических или текущих аспектов. Основные критерии:

- Умение использовать организационные средства, не делая их чрезмерно бюрократическими,
- Эффективно осуществлять взаимодействие с вышестоящими, нижестоящими и равными по рангу сотрудниками
- Умение принимать решения и брать на себя ответственность.
- Понимание языка бизнеса и способность донести ИТ сотрудникам цели бизнеса

Каков бы не был характер человека, руководитель должны иметь опыт работы в ИТ сфере.

Техническая компетентность

Нет ни одного руководителя, техническая подготовка которого была бы столь совершенна, что позволяла бы ему до тонкостей разбираться во всех технических вопросах, возникающих при выполнении сложных ИТ проектов. Однако вы ищете человека, который в состоянии контролировать, оценивать и принимать правильные решения по техническим проблемам, связанным с руководством ИТ направления. Следовательно, должен иметь технический опыт, который состоит в обладании знаниями и навыками как в технической области, так и в области управления, в средствах и умении управлять им.

Требуемая специальная подготовка – и здесь мы фокусируем внимание на инженерных проектах – должна включать в себя:

- Знание по управлению ИТ сервисами
- Знание используемых в управлении проектами
- Знание технических инструментов и методов
- Знание тенденций развития технологии
- Знакомство со смежными техническими областями

Умение работать с людьми

Один из важнейших качеств руководителя – умение общаться с людьми. Руководитель должен уметь:

- заинтересовывать, внушать, ободрять и обучать;
- внимательно выслушивать предложения и поддерживать «обратную связь»
- настойчиво – но не агрессивно или покорно – соотносить с другими и выделять среди других чувства, потребности, заботы и межличностные конфликты;
- предотвращать, а также разрешать конфликты;
- сообщать жесткие решения, даже если они затрагивают интересы других;
- проявлять гибкость – правильно вести себя в различных ситуациях (уметь хорошо играть разные роли).

Признаки умения работать с людьми включают в себя благоприятные отзывы работников, которые работали вместе или под руководством кандидата.

Грамотный руководитель должен знать, чем руководствуется его сотрудник. Можно воспользоваться «Пирамидой Маслоу» для определения потребностей сотрудника:

- Физиологический уровень (еда, дом и т.п.)
- Уровень безопасности (стабильность, защищенность)
- Социальный уровень (дружба, любовь и т.п.)
- Уровень ценности и значимости (уважение, внимание)
- Уровень самореализации (учеба, рост, самовыражение)

Кроме этого при управлении персоналом, желательно принимать во внимание принцип «Теория X и Y менеджеров».

«X менеджмента» – Над сотрудниками необходим постоянный контроль со стороны менеджмента, для сотрудников уровня специалисты и т.п.

«Y менеджмента» – Сотрудники всегда хотят работать, и со стороны менеджмента необходима лишь незначительный контроль для экспертной группы сотрудников.

Руководитель ИТ департамента должен знать основные техники управления коммуникациями:

- Позитивная (Assertive Communication) – создаем условия обоюдного выигрыша
- Пассивная (Passive Communication) – устранение конфликта
- Агрессивная (Aggressive Communication) – использует конфликт для достижения результатов
- Пассивная-агрессия (Passive-Aggressive Communication) – попытка вызвать агрессивное поведение у другого

Доказанные на практике способности к управлению

Прошлое – один из лучших указателей будущего. Способность управлять, очевидно, состоит в том, чтобы получить результат, оставаясь при этом в установленных пределах по финансам,

времени и ресурсам. Чтобы добиться этого, руководитель должен владеть основами управления, то есть понимать, как следует организовывать работу, определять потребность в персонале, формулировать потребности, взаимодействовать с другими уровнями руководства, связывать цель с деятельностью предприятия и, наконец, награждать и наказывать сотрудников.

Ниже перечислены основные навыки, которыми предлагается руководствоваться в работе для эффективного управления и сопровождения проекта:

- Предупреждать события, а не простое реагирование.
- Приступать к работе, помня о конечной цели.
- Делать самое главное в первую очередь.
- Попытаться сначала понять проблему самому, а затем добиться понимания от других.
- Добиваться сплоченности коллектива (целое – это больше, чем сумма составляющих его частей; группа в целом может сделать больше, чем каждый из ее членов).
- Искать компромисс и самосовершенствование.
- Стимулирование участников проекта и нахождение общего языка с ними и другими сотрудниками организации.
- Относиться к сотрудникам с уважением.
- Уметь слушать других.
- Излагать свои взгляды и требования, а также высказывать свое мнение решительно, но не агрессивно.
- Мотивация участников проекта

Рекомендации для руководителя

Для эффективного управления сотрудниками руководить должен выбрать стиль руководства, который мотивирует сотрудников и наделяет их необходимыми полномочиями, а также контролирует и направляет их деятельность:

- Не давать слишком много указаний, избегать чрезмерного надзора и документирования.
- Осознавать различия между сотрудниками. Хорошо знать черты характера, присущие каждому из них.
- Помочь понять суть проблем,
- Оценить творческие возможности и определить, какой вклад они хотели и могли бы внести.
- Предоставить большую свободу действий сотрудникам для выполнения своей работы.
- Быть более терпимым к ошибкам и промахам своих подчиненных.
- Создать благоприятный климат для преодоления трудностей, вызванных неудачами.
- Быть изобретательным и инициативным руководителем, а не надзирателем;
- Быть готовым оказать помощь при возникновении проблем, а не просто раздавать поручения.
- Действовать в качестве буфера между подчиненными и высшим руководством в случае возникновения проблем.
- Непрерывное развитие своих способностей, посещая специальные семинары, читая литературу по специальности и т. п.
- Подавать личный пример своим подчиненным, которому они возможно захотят следовать.

Критерии отбора сотрудников ИТ департамента

Чтобы найти сотрудников, пользуются такими же критериями, как при выборе ее руководителя. Меньший акцент делается на способность к стратегическому мышлению и больший – на конкретную специализацию.

В качестве критериев при выборе сотрудника можно ориентироваться на следующие факторы:

Профессиональные навыки

Для сотрудников уровня «эксперт»:

- экспертные навыки по одному из направлений, наличие опыта работы и сертификации по продукту (например, Microsoft Certified System Engineer + Security в области информационной безопасности по продуктам Microsoft)
- Продвинутые навыки по двум трем смежным направлениям (сетей и сетевых служб Microsoft, виртуализация и т. п.)

- Базовые ИТ знания (основы сети, системы хранения, почтовые системы и т п)

Для сотрудников уровня «инженер / администратор»:

- Продвинутые навыки по одному, двум направлениям, наличие опыта работы и базового уровня сертификации (MCSA)
- Базовые ИТ знания (основы сети, системы хранения, почтовые системы и т п)

Для сотрудников уровня «специалист»:

- Знания по одному, двум продуктам или направлениям, опыта работы и сертификация начального уровня (MCP)
- Базовые ИТ знания (основы сети, системы хранения, почтовые системы и т п)

Персональные навыки

Помимо персональных качеств, для руководителей отделов и групп, необходимо наличие лидерских качеств, умения принимать решения, знать основы Управления ИТ сервисами или проектами, прохождение курсов по навыкам коммуникации, управления временем и т п.

Для сотрудников ИТ подразделения поддержки пользователей, важной является способность к общению, а перечисленные выше характеристики можно использовать и в этом случае, правда, с меньшим акцентом на функции лидера и формального лидера. В качестве рекомендаций можно ориентироваться на следующий список качеств:

- Способность принимать решения
- способность передавать и делить права и ответственность
- гибкость; способность переходить от одного вида работы к другому в зависимости от необходимости
- компетентность в данной области
- готовность признавать ошибки и погрешности и принимать замечания
- ориентированность на выполнение задачи
- способность к пониманию планов и работе в соответствии с графиками и лимитом ресурсов;
- готовность к сверхурочной работе, если необходимо
- способность доверять, помогать другим и принимать помощь
- умение быть игроком в команде, а не героем-одиночкой
- способность работать без и вне формальных иерархий и систем полномочий

Порядок разрешения конфликтов

В процессе функционирования ИТ департамента и взаимодействия с бизнес подразделениями, могут возникать конфликты интересов, как личностные, так и функциональные. Для разрешения конфликтов в организации должен быть разработан и принят процесс разрешения конфликтов. Порядок разрешения конфликтов в ИТ департаменте, если не указан иной, может быть следующий:

- При возникновении конфликта (личностного характера) внутри департамента ИТ между сотрудниками, директор ИТ обязан принять меры по урегулированию конфликта с привлечением обоих сторон
- Если конфликт не удалось урегулировать, ИТ директор обязан привлечь директора департамента Управления Кадрами для совместного урегулирования конфликта
- При возникновении конфликта (личностного характера) между сотрудниками департамента ИТ и сотрудниками других отделов, директор ИТ обязан принять меры по урегулированию конфликта с привлечением главы соответствующего департамента
- Если конфликт не удалось урегулировать, ИТ директор обязан привлечь директора департамента Управления Кадрами для совместного урегулирования конфликта
- При возникновении конфликта (функционального) за пределами ИТ департамента, директор ИТ департамента взаимодействует с главой соответствующего департамента
- Если не удалось разрешить конфликт, то руководители обращаются к департаменту Внутреннего аудита.
- Если и на этом этапе не удалось разрешить конфликт, то он эскалирует на ИТ комитет.

Руководитель ИТ департамента должен уметь управлять конфликтом и знать основные техники, разрешения конфликтов, которые могут оказаться полезными при взаимодействии:

- Совместная работа или сотрудничество (Collaborating)
- Конфронтация или соперничество (Confronting)
- Устранение или избегание (Avoiding)
- Сглаживание, приспособление или поиск компромиссов (Smoothing)
- Давление (Forcing)

Состав и задачи подразделений

Состав подразделений может варьироваться в зависимости от требований и возможностей компании. В данном примере, ИТ департамент состоит из трех подразделений и трех выделенных ролей. Состав подразделения должен включать в себя не менее двух сотрудников, уровня инженер и специалист. Тем самым обеспечивается резервирование сотрудников. Количество сотрудников можно планировать исходя из следующих ограничений: восьмичасовой рабочий день, эффективное время шесть часов, вычитываем один час на личное время (самообразование и т п) и один час на административные операции (регистрация инцидентов и т п). Для сотрудника уровня специалист, половина времени выделяем на выполнения запросов и разрешение инцидентов. Оставшееся время три часа, для стандартного сервиса достаточно для сопровождения порядка шести (6) сервисов. Для сотрудника уровня инженер – выделяем два часа на выполнение запросов. Оставшееся время – четыре часа достаточно для сопровождения порядка 16 сервисов. Все это достаточно условно, и может использоваться как отправная точка для планирования ресурсов. Более точная информация должна быть определена в процессе реальной деятельности ИТ, уровня автоматизации, сложность сервисов, разнородность систем и платформ и т п. Для сотрудников подразделения Поддержки Пользователей планирование сотрудников может исходить из количества сотрудников организации. В зависимости от уровня организации – на одного сотрудника ИТ порядка 50—150 сотрудников организации.

Роль / Позиция	Задачи
ИТ директор	Управление ИТ департаментом, формирование ИТ стратегии и бюджета
Ассистент ИТ директора	Помощь ИТ директору в организационным и административным вопросам
ИТ Архитектор	Формирование ИТ архитектуры, Базовых процедур
ИТ Архитектор Инфраструктуры	Направление по ИТ инфраструктуре
ИТ Архитектор ПО	Направление по Программному Обеспечению.
ИТ Проектный Менеджер	Управление ИТ проектами
Главный специалист по Проектам	Помощь в Управлении ИТ проектами
Ведущий специалист по Проектам	Помощь в Управлении ИТ проектами
Специалист по Проектам	Помощь в Управлении ИТ проектами

Выделенные роли ИТ департамента

Подразделение	Команда	Задачи
CORE Services	Виртуализация Системы Хранения Данных Сети Телефония	Разработка и сопровождение (L2, L3, L4) платформы виртуализации Разработка и сопровождение (L2, L3, L4) платформы СХД Разработка и сопровождение (L2, L3, L4) сетевой инфраструктуры Разработка и сопровождение (L2, L3, L4) телефонии
PRIMARY Services	Windows системы, Linux системы, СУБД	Разработка и сопровождение (L2, L3, L4) Windows платформ Разработка и сопровождение (L2, L3, L4) Linux платформ Разработка и сопровождение (L2, L3, L4) СУБД
SECONDARY Services	Почта + Мессенджер, Портал, Системы мониторинга	Разработка и сопровождение (L2, L3, L4) платформ почты Разработка и сопровождение (L2, L3, L4) платформ мессенджера Разработка и сопровождение (L2, L3, L4) портала Разработка и сопровождение (L2, L3, L4) платформ мониторинга
DEFENSE Services		Разработка и сопровождение (L2, L3, L4) защиты сети Разработка и сопровождение (L2, L3, L4) ОС и приложений

Отдел «Инфраструктуры»

Подразделение	Команда	Задачи
Разработчики	Веб разработчики Программисты Кодеры Веб дизайнеры Программисты БД	Разработка и сопровождение (L2, L3, L4) ПО
Интеграция АСУТП	Электронщики Программисты АСУ	Разработка и сопровождение (L2, L3, L4) ПО АСУТП
Бизнес Приложения Системы Интеграция	Программисты БР Специалисты по БП Специалисты СИ Специалисты по BI	Сопровождение (L2, L3, L4) стороннего ПО Разработка и сопровождение (L2, L3, L4) ПО интеграции Разработка и сопровождение (L2, L3, L4) ПО отчетности
Тестирование ПО		Тестирование ПО, Контроль качества
Бизнес Аналитика		Составление Бизнес Требований, Формирование Технического Задания

Отдел «Разработки ПО»

Подразделение	Команда	Задачи
Информационный центр		Регистрация запросов, инцидентов пользователей, распределение запросов, первая помощь пользователям уровня L0
ИТ поддержка	ИТ Специалисты L1 Техники	Техническая и ИТ поддержка пользователей уровень L1, «Рабочие руки» отделов «Инфраструктуры» и «Разработки ПО»
Обучение пользователей		Подготовка учебного материала, Обучение пользователей, Административные вопросы ИТ департамента

Отдел «Поддержки Пользователей»

Должностные обязанности и ротация сотрудников

Для формирования перечня должностных обязанностей по позициям для ИТ департамента необходимы следующие вводные данные:

- задачи, выполняемые выделенными ролями
- задачи, выполняемые отделами
- ITIL процессы используемые в управлении ИТ
- Используемые технологии и решения
- список предоставляемых ИТ сервисов

Общая иерархия выглядит как:

Включают руководящие функции (непосредственное управление сотрудниками):

- Руководитель департамента
- Руководитель отдела
- Руководитель подразделения
- Лидер группы

Определяют уровень компетенции сотрудника:

- Эксперт
- Инженер / Администратор
- Специалист
- Техник
- Ассистент

Определяют градацию навыков сотрудника или уровень управления:

- Главный
- Ведущий

Наименования позиций в отделе могут меняться в зависимости от специфики использования технических средств. Так для примера %уровень% администратор может быть: главный Windows администратор, ведущий Windows администратор, SharePoint администратор, главный Linux администратор и т.п.

Роль / Позиция	Требования
ИТ директор	Наличие высшего образования, Опыт работы в области ИТ, Опыт руководящей работы
Руководитель отдела	Наличие высшего образования, Опыт работы в области ИТ, Опыт руководящей работы, Опыт работы в компании не менее года, Глубокие ИТ знания, Наличие сертификатов продвинутого уровня
Руководитель подразделения	Наличие высшего образования, Опыт работы в области ИТ, Опыт руководящей работы, Опыт работы в компании не менее года, Глубокие ИТ знания, Наличие сертификатов продвинутого уровня
Лидер команды	Наличие высшего образования, Опыт работы в области ИТ, Опыт руководящей работы, Опыт работы в компании не менее года, Продвинутое ИТ знания, Глубокие ИТ знания по специфическим продуктам и решениям, Наличие сертификатов продвинутого уровня
Эксперт	Наличие высшего образования, Опыт работы в области ИТ, Глубокие ИТ знания, Глубокие ИТ знания по специфическим продуктам и решениям, Наличие сертификатов продвинутого уровня
Главный администратор	Наличие высшего образования, Опыт работы в компании не менее года, Продвинутое ИТ знания, Глубокие ИТ знания по специфическим решениям, Наличие сертификатов продвинутого уровня
Ведущий администратор	Наличие высшего образования, Опыт работы в компании не менее года, Продвинутое ИТ знания, Глубокие ИТ знания по специфическим решениям, Наличие сертификатов начального уровня
Администратор	Наличие высшего образования, Опыт работы в компании не менее года, Продвинутое ИТ знания, Глубокие ИТ знания по специфическим решениям, Наличие сертификатов начального уровня
Главный специалист	Наличие высшего образования, Опыт работы в компании не менее года, Продвинутое ИТ знания, Глубокие ИТ знания по специфическим решениям, Наличие сертификатов продвинутого уровня
Ведущий специалист	Наличие высшего образования, Опыт работы в ИТ более года, Опыт работы в компании не менее года, Продвинутое ИТ знания, Наличие сертификатов начального уровня
специалист	Наличие высшего образования, Опыт работы в ИТ более года, Базовые ИТ знания
Ассистент специалиста	Наличие высшего образования, Опыт работы в ИТ не требуется, Начальные ИТ знания
Техник	Наличие высшего образования не требуется, Опыт работы по своему направлению более года, Базовые знания по своему направлению

Типовые позиции и роли ИТ департамента

При организации ИТ департамента необходимо обратить внимание на вопросы взаимозаменяемости и ротации сотрудников ИТ департамента. Определяет процесс подчинения и возможности взаимозаменяемости ИТ сотрудников. Правильно выстроенная система позволяет оптимизировать количество сотрудников и поддерживать высокий уровень качества предоставления ИТ сервисов при кратковременном отсутствии сотрудников ИТ. Структура поддерживает иерархическую связь т.е. наследование подчинения при отсутствии или вакантной позиции. Так для примера связь «сверху вниз» главный ИТ администратор заменяет ведущего ИТ администратора, который в свою очередь заменяет ИТ администратора. При отсутствии ведущего ИТ администратора, главный ИТ администратор заменяет ИТ администратора. Тот же принцип сохраняется при связи «снизу вверх». Как пример:

Роль / Позиция	Непосредственный руководитель	Заменяет
ИТ директор	Совет директоров	Руководитель отдела
Ассистент ИТ директора	ИТ директор	
Руководитель отдела	ИТ директор	Руководитель подразделения, Лидер команды
Руководитель подразделения	Руководитель отдела	Лидер команды
Главный ИТ администратор	Руководитель подразделения	Ведущий ИТ администратор
Ведущий ИТ администратор	Руководитель подразделения	ИТ администратор
ИТ администратор	Руководитель подразделения	Главный ИТ специалист
Главный ИТ специалист	Руководитель подразделения	Ведущий ИТ специалист
Ведущий ИТ специалист	Руководитель подразделения	ИТ специалист
ИТ специалист	Руководитель подразделения	Ассистент ИТ специалиста
Ассистент ИТ специалиста	Руководитель подразделения	N/A

Обучение сотрудников

Определяет процесс роста персональных и технических навыков сотрудников ИТ департамента. Правильно выстроенная система позволяет поддерживать высокий уровень качества предоставления ИТ сервисов. Ключевые аспекты включают в себя, но не ограничиваются ниже перечисленными:

- Обязательно выделять статью в бюджете на обучение сотрудников ИТ
- Процесс должен носить регулярный и повторяющийся характер

Формы и виды обучения:

- Самообучение, используя обучающие материалы, книги и т п
- Внутренние семинары в ИТ департаменте. Передача опыта более опытными сотрудниками в департаменте. Ответственный за организацию несет директор ИТ департамента.
- Внутренние семинары общего значения. Обучение внутри организации. Проводимые внутренними департаментами компании, не имеющие технической направленности. Например, со стороны Отдела Кадров – правила работы в компании, коммуникация с сотрудниками и т п, со стороны департамента безопасности – общие правила по информационной безопасности и т п). Как правило организуется со стороны отдела кадров.
- Обучение сотрудников на специализированных курсах.

Ответственный за организацию несет директор ИТ департамента.

Основные шаги обучения сотрудников стоятся по принципу: Слушать, Чтение материала, Наблюдение и Выполнение.

Согласно материалам «NT: Institute for Applied Behaviours Science» результативность различных подходов обучения:

- Слушать 5%
- Чтение материала 10%
- Наблюдение 25%
- Выполнение 75%

Порядок обучения сотрудников желательно строить по принципу:

- Прохождение курсов (получение теоретических знаний)

- Практика эксплуатации системы (получение практических навыков работы)
- Прохождение международной сертификации (получение признания сторонних организации)

Роль / Позиция	Количество курсов в год	Разрешенный Бюджет
ИТ директор	Не ограничивается	Не более 20% бюджета
Руководитель отдела	До 7 внешних курсов или семинаров, Бесплатные семинары не ограничено	4000 манат
Руководитель подразделения	До 7 внешних курсов или семинаров, Бесплатные семинары не ограничено	4000 манат
Эксперт	Не ограничивается	Не более 10% бюджета
Главный администратор	До 5 внешних курсов или семинаров, Бесплатные семинары не ограничено	3000 манат
Ведущий администратор	До 4 внешних курсов или семинаров, Бесплатные семинары не ограничено	2000 манат
Администратор	До 4 внешних курсов или семинаров, Бесплатные семинары не ограничено	2000 манат
Главный специалист	До 3 внешних курсов или семинаров, Бесплатные семинары не ограничено	2000 манат
Ведущий специалист	До 2 внешних курсов или семинаров, До 3 бесплатных семинара	1500 манат
специалист	До 2 внешних курсов или семинаров, До 3 бесплатных семинара	1000 манат
Ассистент специалиста	Не предусмотрены	Не предусмотрены

*- Предполагается внешний курс является платной услугой и включает в себя 40 часов стоимость порядка 500 манат.

Порядок организации процесса обучения в ИТ департаменте:

- Работники отделов ИТ в течении года отправляют своему непосредственному руководителю список курсов, которые хотели бы посетить на следующий год. Количество курсов определяется в зависимости от позиции сотрудника и распределённого бюджета на обучение. Может выражаться как в абсолютных (3 курса, 1000 манат), так и относительных величинах (в два раза больше, 10% от бюджета и т п).

- Руководитель отдела определяет необходимость в данных курсах. Курсы должны быть направлены на продукты, которые используются или планируется использовать в ИТ архитектуре и иметь отношение к работе сотрудника.

- ИТ директор обобщает список курсов всего департамента, корректирует при необходимости, и формирует бюджет на обучение на следующий год.

- После одобрения бюджета, ИТ директор корректирует список по необходимости, и информирует руководителей отделов.

- ИТ директор дает указание на отправку списка курсов и предполагаемое количество сотрудников для поиска предложений.

- После получения предложений, формируется график посещения курсов.

- После прохождения курсов, сотрудник обязан не позднее двух недель подготовить и провести внутренний семинар для сотрудников ИТ департамента. Это позволит определить уровень усвоения материала, а также повысит осведомлённость всего ИТ департамента.

- Материалы передаются в ИТ департамент (или общую библиотеку если таковая имеется) для пополнения базы знаний.

- Если по окончанию запланированных курсов остается бюджет, он может быть использован для прохождения дополнительных курсов (покупку учебных материалов и т п) по усмотрению директора ИТ.

- Директор ИТ департамента несет ответственность за то, чтобы бюджет не был превышен.

- Бюджет на обучение не может быть перенесен на другие цели, кроме как обучение.

- Бюджет на сотрудника не переносится на следующий год, а формируется заново (т. е., например, если сотруднику положено 2 курса в год общей стоимостью 1000 манат и в этом году он не прошел курсы, то на следующий год его лимит остается тем же, а не увеличивается до 4-х курсов т 2000 манат).

•Посещение бесплатных семинаров сотрудником возможно только с разрешения руководителя отдела.

Мотивация и премирование сотрудников

Определяет процесс мотивации и премирования сотрудников ИТ департамента. Правильно выстроенная система позволяет поддерживать высокий уровень лояльности сотрудников и как следствие высокий уровень качества предоставления ИТ сервисов.

Премирование сотрудников может происходить, но не ограничиваться в следующих случаях:

- Получение международного сертификата в своей области
- Выполнение проекта (создание новых программных продуктов и т п) на условиях удобных бизнесу.
- Выполнение дополнительных работ (разворачивание филиала и т п) на условиях удобных бизнесу.
- Достижения компанией положительных результатов (квартальная, полугодовая или годовая премия и т п)

Основные моменты:

- Премирование может носить разовый и/или регулярный характер.
- При премировании используется принцип наследования. Т. е., например, при прохождении сертификации по продукту Microsoft SQL (MCITP DBA) автоматически вы получаете сертификат MCITP общий. В таких случаях оплачивается один сертификат.
- Политика премирования за отдельные проекты и сертификаты не распространяется на директора ИТ департамента. Как руководитель «С Level» уровня он оценивается руководством компании за всю работу департамента, обычно ежегодная премия.

Помимо всего выше перечисленного необходимо выделять статью бюджета, или иметь готовый процесс со стороны отдела кадров, на проведение встреч по формированию команды «Team Building», представительские расходы (встречи гостей и т п,) для обмена опытом и т п.

Для примера может использоваться следующая таблица.

Статья премирования	Сумма
Получение сертификата начального уровня (MCP, A+, ITILv3, MCTS, CCENT). Стоимость премии превышает расходов на прохождение сертификации. Для получения сертификата достаточно прохождения одного экзамена.	500 манат
Получение сертификата среднего уровня (MCSA, Network+, Security+, VCP, CCNA, CEH, ECSA, MCITP, MCITP DBA, SCSP). Стоимость премии превышает расходов на прохождение сертификации. Для получения сертификата необходимо прохождение двух и более экзаменов или стоимость экзамена превышает стоимость премии.	1000 манат
Получение сертификата высокого уровня (MCSE, CCNP, LPT, MCT, CISA, CISSP, CAMP, ITILv3 Expert). Стоимость премии превышает расходов на прохождение сертификации. Сертификат имеет высокую стоимость и ценность.	1500 манат
Получение сертификата уровня мастера (MCM, CCIE, MCA, CCIA, PMP, ITILv3 Master). Стоимость премии превышает расходов на прохождение сертификации. Сертификат имеет высокую стоимость и ценность.	2000 манат
Разворачивание небольшого филиала (не более 200м2). Объем работ предполагает работу двух-трех ИТ специалистов в течении двух дней.	Бюджет 800 манат, или два дня отпуска каждому работнику
Разворачивание небольшого филиала (не менее 200м2, но не более 500м2). Объем работ предполагает работу трех ИТ специалистов в течении двух дней.	Бюджет 1000 манат, или три дня отпуска каждому работнику
Разворачивание небольшого филиала (более 500м2). Объем работ предполагает работу трех-четырех ИТ специалистов в течении двух дней.	Бюджет 1500 манат, или четыре дня отпуска каждому работнику
Полугодовая / годовая оценка сотрудника	50-100% зарплаты

Градация и продвижение сотрудников

Определяет процесс роста и развития ИТ персонала в компании. Правильно выстроенная система позволяет поддерживать высокий уровень лояльности сотрудников, снизить текучесть

кадров, поддерживать высокий уровень мотивации, персональные и технические навыки сотрудников.

Градация уровней позволяет использовать механизмы при формировании зарплаты сотрудникам.

ИТ Специалист, проработавший в данной компании, более важен компании чем ИТ специалист с теми же навыками, но только прибывший. Это связано с тем, что, хотя технические навыки у каждого равные, но первый знаком с правилами работы в компании, организацией, методами, используемыми в ИТ и т.п. что в конечном плане, влияет на эффективность работы.

в силу влияния персональных качеств, тот или иной работник одной позиции может иметь разную ценность для компании.

Основные составляющие при формировании системы градации могут служить:

- Наличие высшего образования
- Наличие опыта работы в ИТ
- Уровень знаний по продуктам и решениям (набор или повышение, определяет тесты или аттестация)
- Наличие опыта и срок работы в ИТ в данной организации (повышение)
- Персональные качества
- Уровень знаний процедур и процедур (повышение, определяется при аттестации)
- Наличие сертификатов и их уровень
- Количество часов пройденных курсов
- Наличие благодарностей со стороны руководства (повышение)

Тестирование и аттестация сотрудников

Процесс оценки персональных и технических навыков сотрудников ИТ департамента как при наборе (тестирование), так и при повышении (аттестация). Правильно выстроенная система позволяет поддерживать высокий уровень качества предоставления ИТ сервисов.

Ключевые аспекты включают в себя, но не ограничиваются ниже перечисленными:

- Наличие тестов при проведении набора в ИТ для оценки технических навыков.
- Наличие тестов при проведении набора в ИТ для оценки персональных навыков.
- Наличие процедуры проведения отбора сотрудников.
- Наличие тестов для проведения аттестации ИТ сотрудников на оценку технических навыков.
- Наличие тестов для проведения аттестации ИТ сотрудников на оценку знания политик и процедур.

Общий вид процесса отбора ИТ персонала может выглядеть как:

•Первый этап – отдел кадров формирует опросник (порядка 20 вопросов из базы вопросов, предоставленных департаментом ИТ). Этому предшествует сбор резюме и заявок в течении двух трех недель. Кроме этого в состав теста добавлены общие вопросы (порядка 10 вопросов математика, логика психология и т.п.). Сотрудник отдела кадров проводит тестирование с соискателями. Присутствие представителя ИТ департамента необязательно. Определяется пороговое значение для прохождения (например, 60%). На тесты выделено порядка 30 минут.

•Второй этап – отдел кадров и представитель ИТ департамента проводят интервью с соискателями прошедших тестирование (через одну неделю после тестов). На данном этапе имеется резюме и результаты теста соискателя. Представитель ИТ департамента проводит интервью на основе опросника для оценки глубины технических знаний и отсутствие подлога в результатах теста. На каждого соискателя выделяется порядка 30 минут. По результатам интервью формируется список «рекомендуемых» кандидатов (порядка трех человек по рейтингу).

•Третий этап – встреча с руководителем ИТ департамента и руководителем отдела кадров (через неделю после интервью). Этому предшествует работа департамента безопасности и отдела кадров, по проверке потенциальных кандидатов. На финальном этапе делается предложение кандидату или отказ, определяют, когда кандидат может начать работать. Отдел кадров ожидает по необходимости ответ соискателя (но не более недели). В случае положительного решения,

отдел кадров сообщает руководителю ИТ департамента, когда кандидат приступит к работе и закрывает вакансию.

Для обеспечения прозрачности и контроля процесса набора сотрудников желается производить регистрацию в течении всего процесса. Также желательно иметь базу кандидатов (прошедших, не прошедших, поданные заявки и резюме). Для оптимизации процесса отбора персонала, желательно определить период, в течении которого кандидат, не прошедший тесты или интервью, может повторно падать на вакансию в организации (как правило от шести месяцев до года). При наборе сотрудников, можно определить позиции, на которые можно производить внешний набор, а для каких желательно использовать внутренние ресурсы. Исключение может составлять случае, когда формируется новый департамент, отдел или подразделение.

Как пример можно использовать следующую матрицу

Позиция	Принятие на работу	Повышение
Руководитель отдела Руководитель подразделения	N/A	Рекомендация руководителя, Аттестация раз в три года, Технические навыки, Знание политик и процедур отдела Знание политик и процедур компании
Лидер команды Главный администратор	N/A	Рекомендация руководителя, Аттестация раз в два года, Технические навыки, Знание политик и процедур отдела
Эксперт	Собеседование Тест на профпригодность Тест персональных качеств	Рекомендация руководителя, Аттестация раз в три года, Технические навыки, Знание политик и процедур отдела
Ведущий администратор Главный специалист Ведущий специалист Главный техник Ведущий техник	N/A	Рекомендация руководителя Аттестация раз в год: Технические навыки Знание политик и процедур отдела
Администратор Специалист Ассистент специалиста Техник Ассистент техника	Собеседование Тест на профпригодность Тест персональных качеств	Рекомендация руководителя Аттестация раз в год: Технические навыки Знание политик и процедур отдела

Для качественной и количественной оценки сотрудника можно ввести систему оценки, которая помогает организации определить достижение стратегических и тактических целей. Использование ключевых показателей эффективности даёт организации возможность оценить своё состояние и помочь в оценке реализации стратегии.

KPI – это инструмент измерения поставленных целей. Если показатель, который вы придумали, не связан с целью, то есть не образуется исходя из её содержания, тогда нельзя использовать данный термин. Преимущества методики – наличие прозрачной системы оценки работы предприятия. Она состоит из показателей и их целевых значений, установленных для каждого сотрудника, списка мероприятий для достижения планового уровня KPI с указанием сроков их выполнения, расшифровки методики расчета по показателям, перечня лиц, которые будут проводить оценку. Такая система позволяет руководству отслеживать в динамике эффективность деятельности каждого подразделения и сотрудника, прогнозировать результаты работы компании за год.

Возможность корректировки действий сотрудников в течение года в случае, если результаты их работы не достигают до запланированных уровней. Объективность оценки работы сотрудников. Конечно, в случае оценки деятельности работников вспомогательных подразделений, или представителей творческих профессий (дизайнеры и т п) не всегда удастся установить количественные показатели. В таком случае применимы качественные. Для эффективной работы методики необходимо создание системы обратной связи, позволяющей специалисту оперативно получать оценку своей деятельности на основе объективных критериев, а не общего впечатления, сложившегося у начальника. Система премирования на основе KPI

способствует мотивации персонала к повышению производительности и достижению стратегических целей компании, а также позволяет обосновать размер премии. Плановый уровень бонуса определяется, как правило, в виде процента от оклада работника. Конкретный процент зависит от уровня должности и профиля деятельности сотрудника.

Для успешного внедрения KPI следует объяснить сотрудникам предназначение системы, механизм ее работы, преимущества для организации и персонала. Кроме того, нередко нужны специальные тренинги по управлению эффективностью для отдела кадров и руководителей всех уровней. Все это требует не только определенных денежных вложений, но и грамотного исполнения.

Лучше не заниматься системой KPI вообще, нежели внедрить неудачно и тем самым дискредитировать ее в глазах сотрудников, которые при следующих попытках наладить работу системы будут относиться к технологии с недоверием.

Следует обратить внимание, что затраты на внедрение технологии окупаются в первую очередь на средних и крупных предприятиях, где необходимо обеспечить прозрачность системы управления. В случае небольших компаний, где начальник может контролировать деятельность сотрудников без дополнительного сложного инструментария, затраты на внедрение могут себя не оправдать либо вообще, либо по крайней мере в первые годы работы системы.

Рекомендации по эффективному управлению персоналом

Можно привести еще много рекомендаций и критериев при отборе сотрудников, но важно помнить несколько «законов жизни»:

- Выбор сотрудника – это всегда в какой-то степени лотерея. Надо быть немного везунчиком
- Математика и подсчет «попугаев» (галочек в чек листе) не всегда может помочь. Одно гнилое яблоко в вазе со свежими яблоками не станет свежим со временем, а вот то, что все остальные яблоки в вазе также сгниют – факт.
- Нанимая молодого руководителя с прекрасными знаниями, но без достаточного опыта, вы оплачиваете не только его знания, но и те ошибки, которые он совершит.
- Организация несет больше всего убытков в двух случаях – если сотрудник вор, или если сотрудник дурак.
- Не убивайте мотивацию сотрудников. Поощрение новаторских идей, и доведение их до сведения начальства, и настройка механизма обратной связи. Без обратной связи поток творческих идей иссякнет, поскольку новаторы будут считать, что их идеям не уделено должного внимания или они не воспринимаются серьезно.

Современная методика DevOps

На сегодняшний день, помимо представленных выше классических методов организации деятельности ИТ имеется также и альтернативные решения. Один из вариантов представляет из себя методология DevOps (Development & Operations). Методология находится на стыке разработки и операционного управления.

Сама по себе методология DevOps – это не просто набор техник, это философия современного управления ИТ деятельностью. Ее появление связано с изменениями в технологиях за последнее время. По большей части это связано с тем, что организации переходят от классических приложений к быстрой разработке, тестированию, введению в эксплуатацию и сопровождению решений. Это требует быстрой реакции и тесного взаимодействия ИТ подразделений между собой.

Переход к DevOps призван уменьшить число конфликтов, возникающих, когда разработчики ориентированы на удовлетворение требований бизнеса, добавление новых функций, удобства использования и т.п., а ИТ специалисты традиционно сосредоточены на надежности, безопасности и доступности функционирования ИТ систем. Таким образом, разработчиков нужно учить операционной деятельности, а эксплуатационников – более быстрому и эффективному удовлетворению потребностей бизнеса. Понимание и согласованность действий разработчиков и ИТ специалистов по сопровождению будет способствовать уровню удовлетворенности клиентов.

Основополагающая техническая концепция DevOps: по мере автоматизации процессов взаимодействия с инфраструктурой в ходе построения, тестирования, развертывания

и мониторинга ИТ организации могут устранить многие операционные дефекты и улучшить разработку и сопровождение решений. На практике, основные вопросы заключаются в том, как и какие инструменты следует использовать по каждой отдельной области DevOps.

На мой взгляд, можно провести аналогию, по которой DevOps можно рассматривать как гибкой «Agile» методикой организации ИТ деятельности. Как и в управлении проектами, данная методика имеет свои плюсы и минусы, и ей еще предстоит доказать свою эффективность в течении времени.

Перечень и формат руководящих ИТ документов

Руководящие документы по управлению ИТ, для удобства, различаются по следующим категориям:

ИТ устав и политики – высокоуровневые документы, определяющие общие положения, методы достижения целей и т п. Определяют высокоуровневые значения (например, ... длинна пароля должна быть регламентирована ...).

ИТ Стандарт – документы промежуточного уровня, определяющие метрики для методов, определённых в политиках (например, ... длинна пароля восемь символов...).

ИТ Процедуры и планы – документы промежуточного уровня, определяющие пошаговый регламент работ для применения политик с использованием метрик стандартов, инструменты, исполнителей, инструкций и т п.

ИТ Инструкции и акты – низкоуровневые документы, определяющие инструкции для сотрудников внутри ИТ департамента, конечных пользователей, факты выполнения тех или иных действий и т п.

Уровни управления	Название	Действия	Степень детализации
Стратегический	Стратегия ИТ	Вопрос «Что делать?»	Низкая
Тактический	Архитектура ИТ	Вопрос «Как делать?»	Средняя
Операционный	ИТ-процессы ИТ-проекты	Выполнять!	Высокая

Диаграмма: Уровни управления, задачи и детализации

Для удобства организации работы ИТ и снижения административной нагрузки можно принять за правило (если это не противоречит правилам компании), что, все высокоуровневые и промежуточные документы необходимо подтверждать на ИТ комитете, а низкоуровневые документы могут быть разработаны и утверждены директором ИТ департамента.

Структура устава ИТ департамента может содержать следующие пункты:

Общие положения

Цели документа

Принятые сокращения и определения

Сфера действия документа

Организации работы с документом (разработка, внедрение, утверждение и т п)

Цели ИТ департамента

Задачи ИТ департамента

Функции ИТ департамента
Структура ИТ департамента
Роли и ответственности
Порядок взаимодействия
Порядок разрешения конфликтов
Показатели эффективности и критерии оценки деятельности
Контроль документа
Контроль версии документа

Базовый формат политик ИТ департамента может содержать следующие пункты:

Общие положения
Цели документа
Принятые сокращения и определения
Сфера действия документа
Порядок организации документа (разработка, внедрение, утверждение и т.п.)
Связанные документы и политики (процессы)
Влияние при отсутствии документированной политики (процесса)
Цели политики (процесса)
Задачи политики (процесса)
Процессы и процедуры
Под-процесс 1 (процедура 1)
Под-процесс 2 (процедура 2)
Под-процесс N (процедура N)
Метрики политики (процесса)
Роли и ответственности
Порядок взаимодействия политики (процесса)
Риски при внедрении и сопровождении политики (процесса)
Ключевые факторы успеха внедрения и сопровождения политики (процесса)
Показатели эффективности и критерии оценки деятельности политики (процесса)
Отчетность по политике (процессу)
Контроль документа
Контроль версии документа

Детальная Архитектура ИТ сервиса может содержать следующие пункты:

Название
Назначение
Требования
Ограничения
Архитектура (физическая и логическая)
Инфраструктура
Зависимости и окружения
Лицензирование
Мощности
Масштабирование
Отказоустойчивость и восстановление
Резервирование
Архивирование
Система обновления
Роли и ответственности
Оценка рисков
Тестирование

Внедрение
Установка
Конфигурирование
Сопровождение
Стандартные Операционные Процедуры
Требования к сотрудникам
Стоимость
Индикаторы производительности
Аудит и контроль логов
Мониторинг и метрики сервиса
Управление
Отчетность
Рекомендации
Выводы и уроки
Дополнения и замечания

Документ может быть разбит на две части: архитектура сервиса и руководство по операционной деятельности.

Для идентичных действий (например, порядок разработки, внедрение, утверждение, нумерации и т.п.) можно использовать отдельный документ по данному процессу, и соответственно исключить данную секцию из документа.

Для небольших организаций, организаций с вялотекущими ИТ процессами, или незначительным влиянием ИТ на бизнес допускается совмещение политик, процедур и стандартов различных процессов в едином документе.

Ведение документации один из важнейших элементов административной работы и управления. Никто не любит писать документы... кроме тех, кто умеет. Используйте готовые шаблоны и отчетные формы. Но перед тем как начинать придумывать или заполнять готовые шаблоны, нужно ответить на три важных вопроса:

- Какие документы нужны для вашей организации сейчас?
- Насколько детально нужно их прорабатывать?
- Стоимость времени, потраченное на создание документа по отношению к ценности документа?

Генерировать кучу ненужных документов дорого, долго и глупо. Это выгодно, если проект оценивают по толщине отчетных документов. Но толстые документы никто не читает. Их ставят на самую дальнюю полку и забывают навсегда. Поэтому нужно выбрать только те документы, которые нужны для достижения целей проекта. Для результатов. И прорабатывать их настолько детально, насколько это нужно для достижения целей. Логично. Но как определить эту грань? Так как разработка документации и административные работы требуют дополнительных ресурсов, порядок разработки и глубина проработки ИТ документации может быть различной как для различных организаций, так и отдельных процессов в одной организации.

Различают важность документов по следующим типам:

По степени важности

- Устав, планы, бюджет и т.п.
- Политики
- Стандарты
- Процедуры
- Прочие документы

По уровню взаимодействия

- Взаимодействие ИТ департамента с внешними организациями
- Взаимодействие ИТ департамента с подразделениями внутри организации
- Взаимодействие внутри ИТ департамента

Можно руководствоваться различными методами внедрения:

«Классический» – разрабатывается документация и процессы собственными силами или с привлечением консультантов и экспертной группы. Внедрение поэтапное основных и второстепенных процессов.

Достоинства:

- Наиболее правильный с точки зрения организации
- Проработана цепочка «снизу – вверх» и «сверху-вниз»

Недостатки:

- Достаточно затратный как в финансовом, так и во временном плане
- Не эффективен в условиях ограниченных ресурсов

«По требованию» – процессы формируются в ходе внедрения и сопровождения ИТ сервисов. Далее происходит их обкатка, и лишь затем формальное документирование, и принятие. Приоритеты также формируются по необходимости. Так, например, в первую очередь прорабатываются процессы взаимодействия ИТ и внешней организации (поставщиками продуктов, компанией разработчиками и т.п.). На следующем уровне организуются процессы взаимодействия ИТ департамента с другими подразделениями компании. И в последнюю очередь формализуется организация работ внутри самого ИТ департамента.

Достоинства:

- Эффективен с точки зрения использования ресурсов
- Простота и понятность в организации простых процессов
- Целевой, направлен на управление наиболее важными «живыми» процессами в организации, а не формально «важными» с точки зрения управления ИТ сервисами

Недостатки:

- Является реактивным методом, т.е. работает по факту происходящих действий
- Требует дополнительного времени и ресурсов по интеграции процессов между собой

Техника «постепенного улучшения», которая представляет из себя следующую последовательность действий:

- Сначала берете (или выбирается) минимальный набор документов.
- Заполняете на основании здравого смысла. Если что-то кажется лишним, отбрасывайте.
- Затем оцениваете, сможете ли вы с помощью этой информации достичь нужных результатов.
- Если нет, то включите недостающие разделы или документы.
- Заполните их и снова проведите оценку.
- И так далее до достижения результатов.

Выбор метода зависит от индивидуальных особенностей организации и ее культуры, на мой взгляд использование метода «по требованию» с применением техники «постепенного улучшения» является наиболее удачным.

Процедура утверждения руководящих ИТ документов в общем случае может выглядеть так:

- Для процессов, владельцем которых является ИТ, утверждение возможно по решению ИТ директора

- Разрешение конфликта интересов происходит согласно процедуре в два этапа: инициатор и ИТ директор привлекают департамент Аудита. Если конфликт не разрешен, то запрос направляется на ИТ комитет.

- Для процессов, владельцем которых ИТ не является, утверждение возможно только по решению ИТ комитета

- Ряд документы требует разработку их в других департаментах. При этом соблюдается алгоритм действий:

- ИТ ссылается на документ, разработанный в соответственном функциональном департаменте (документы по кадрам, закупкам и т п). Если документ отсутствует в функциональном департаменте, то ИТ разрабатывает его самостоятельно по вопросам, связанным с ИТ с учетом вербальных требований функционального департамента.

Для предоставления качественного ИТ сервиса необходимо разработать и внедрить следующие виды документов:

- Устав ИТ департамента (01)
- Политики и положения (02)
- Стандарты (03)
- Процедуры (04)
- Планы и бюджеты (05)
- Должностные инструкции (06)
- Сервисные соглашения SLA & OLA (07)
- Инструкции и руководства (08)
- Акты и формы (09)
- Отчеты (10)
- Прочие документы (11)

Маркировка и именование ИТ активов

Схема именования ИТ активов предоставляет возможность структурировать организацию ИТ активов. Схема именования может отличаться от компании к компании. Она может отображать расположение оборудования, принадлежность к филиалу, тип оборудования, его назначение, серийный или порядковый номера и т п. Желательно иметь документацию определяющую порядок маркировки и именования элементов. Желательно чтобы полный набор не превышал 15 символов. Как пример можно рассмотреть следующую схему именования объектов:

Маркировка серверов

ABCD-KLM-XYZ12

ABCD: определяет ИТ сервис (например ADS, DHCP, RDP и т п). Может состоять из трех, четырех символов.

KLM: определяет расположение или принадлежность компании (PDC, SDC и т п). Может состоять из трех, четырех символов.

XY: определяет роль данного сервера в предоставляемом ИТ сервисе (например DC, FDC, MS, DA и т п). Может состоять из двух, трех символов.

12: определяет порядковый номер сервера с данной ролью. Может состоять из двух символов.

Примеры: ADDS-PDC-FDC01, ADDS-PDC-DC01, DHCP-PDC-MS01, RDP-PDC-WA01, SPS-PDC-DB01

Маркировка сетевого оборудования

AB-KLM-WXYZ-12-34

AB: определяет тип устройства (например SW, RT, GW и т п). Может состоять из двух, трех символов.

KLM: определяет расположение или принадлежность компании (PDC, SDC и т п). Может состоять из трех, четырех символов.

WXYZ: определяет роль устройства (например CORE, DSTR, ACCS и т п). Может состоять из трех, четырех символов.

12—34: определяет порядковый номер устройства с данной ролью или этаж. Может состоять из двух, четырех символов.

Примеры: SW-PDC—CORE-01, SW-PDC-ACCS-01, AP-PDC-ACCS-01-01

Маркировка систем хранения, резервного копирования и архивирования данных

ABCD-KLM-WXYZ12

ABCD: определяет тип устройства (например STRG, TAPE и т п). Может состоять из трех, четырех символов.

KLM: определяет расположение или принадлежность компании (PDC, SDC и т п). Может состоять из трех, четырех символов.

WXYZ: определяет роль устройства (например MAIN, BACKUP, ARCH и т п). Может состоять из трех, четырех символов.

12: определяет порядковый номер устройства. Может состоять из двух символов.

Примеры: ST-PDC-MAIN01, ST-PDC-BACKUP01

Маркировка систем конечных пользователей

AB-KLM-XY123456789

AB: определяет тип устройства (например WS, LT и т п). Может состоять из двух, трех символов.

KLM: определяет расположение или принадлежность компании (PDC, SDC и т п). Может состоять из трех, четырех символов.

XY123456789: определяет порядковый или серийный номер устройства.

Примеры: WS-PDC-AV201736454, LT-SDC-00001

Маркировка офисной техники

ABCD-KLM-XY-123456789

ABCD: определяет тип устройства (например PRNT, COPR и т п). Может состоять из двух, трех символов.

KLM: определяет расположение или принадлежность компании (PDC, SDC и т п). Может состоять из трех, четырех символов.

XY-123456789: определяет порядковый или серийный номер устройства, этаж расположения или тип.

Примеры: PRNT-PDC—CL-201736454, COPR-SDC-BW-00001, COPR-SDC-1F-00001

Маркировка объекта активного каталога «Организационная единица»

ABCD

ABCD: определяет ИТ сервис (например ADS, DHCP, RDP и т п). Может состоять из трех, четырех символов.

Маркировка объекта активного каталога «Группа»

ABCD-XY-WZ

ABCD: определяет ИТ сервис (например ADDS, DHCP, RDP и т п). Может состоять из трех, четырех символов.

XY-WZ: определяет роль или задачи группы (например ADM, R, RW, DATA-ACCESS и т п).

Примеры: FSS-ADM, RDP-ADM, DHCP-READ, SPS-DATA-CCESS

Маркировка объекта активного каталога «Сервисная учетная запись»

ABCD- KLM – XY-12

ABCD: определяет ИТ сервис (например ADS, DHCP, RDP и т п). Может состоять из трех, четырех символов.

KLM: определяет тип учетной записи (SVC фиксированный для gMSA или USR для пользовательской). Может состоять из трех фиксированных символов.

XY: определяет роль или задачи учетной записи (например ADM, READ, DATA-ACCESS и т п).

Примеры: FSS-SVC-BACKUP, RDP-USR-ADM, SPS-SVC-DATA-ACCESS

Маркировка объекта активного каталога «Пользователь»

ABCD. KLM. XY

ABCD: определяет имя пользователя написанное на английском с применением таблицы символов. Может состоять из трех, четырех символов.

KLM: определяет имя пользователя написанное на английском с применением таблицы символов.

XY: определяет имя пользователя написанное на английском с применением таблицы символов. Может состоять из одного или двух символов. Используется только в случае имеющегося полного совпадения.

Примеры: Vadim. Aldzhanov, Mammad.Mammadov, Mammad. Mammadov. R

Маркировка дополнительных элементов

К дополнительным элементам, требующим маркировку можно отнести следующие:

- Именованное помещений
- Маркировка рабочих точек
- Координатная сетка ЦОД
- Маркировка коммуникационных и коммутационных шкафов
- Маркировка пассивных элементов СКС
- Порядок именования ИТ сервисов
- Порядок именования ИТ документации

Заключение

Организация управления ИТ департаментом является одной из важнейших составляющих при построении ИТ архитектуры. Главные составляющие:

- Сотрудники – должны быть мотивированны и обучены.
- Процессы – должны быть простые для понимания и исполнения.
- Документация – должен присутствовать необходимый минимум для регулирования деятельности сотрудников и процессов.

Компоненты ИТ Инфраструктуры Общие Положения

В данной главе рассмотрены компоненты ИТ инфраструктуры. На иллюстрации можно видеть основные компоненты.



Платформа вычислений

Платформа вычислений – ядро ИТ инфраструктуры, представляет из себя набор систем и решений, представляющие из себя стратегические ИТ активы технологической архитектуры. Как пример, ядро ИТ инфраструктуры предприятия может представлять из себя следующие решения или их комбинации:

- физические сервера
- платформа виртуализации
- платформа облачных вычислений
- гибридные решения



Как пример, платформа вычислений с применением виртуализации на базе решения VMware размещенная по схеме «on-premise», может содержать следующие элементы:

- Аппаратное обеспечение (физические сервера)
- Гипервизоры (программное обеспечение)
- Система Хранения Данных (СХД)
- Сетевая Инфраструктура
- Система Управления и Конфигурации (например, vSphere)
- Система Мониторинга (например, vSphere и т п)

Платформа коммуникации

Платформа коммуникации – второй компонент ИТ инфраструктуры, призванные обеспечить взаимодействия всех компонентов. Как пример, может включать в себя:

- Протоколы и технологии LAN/WAN/Data Center Network
- Коммутаторы ядра, распределения и доступа
- Маршрутизаторы
- Балансировщики нагрузки

Как пример, платформа коммуникации для платформы виртуализации на базе аппаратных решений, размещенных по схеме «on-premise», может содержать следующие элементы:

- Ядро коммутации (Ethernet коммутатор L2/L3), для доступа к подсети управления и доступа виртуальных машин
- Коммутаторы системы хранения (SAN switch), предназначенные для связи гипервизоров и системы хранения данных
- Коммутаторы уровня распределения и доступа
- Маршрутизаторы и контроль доступа

Следующий уровень компонентов можно условно разделить на три группы:

- Технические системы – ИТ

- Системы общего назначения
- Бизнес Системы

Технические системы

Технические системы – ИТ системы и решения, предназначенные для развертывания и сопровождения ИТ инфраструктуры и обеспечения функционирования систем общего назначения и Бизнес Систем. Как пример, Активный каталог, системы централизованного управления и мониторинга, службы DNS, DHCP и т.п.

Системы Общего Назначения – ИТ решения, предоставляющие базовые ИТ сервисы. Базовые требования к системам по большей части известны. Как пример решений – предоставление общего доступа к файлам, службы централизованного управления печатью, почтовые системы и системы передачи мгновенных сообщений и т.п.

Бизнес Системы

Автоматизированные Системы Управления

Бизнес Системы – системы, основное предназначение которых обеспечить выполнения бизнес требований. Как пример – различные ERP, CRM системы. В отличие от систем общего назначения, требования к функционированию и возможностям систем ставятся со стороны бизнеса.

Основная задача ИТ является в планировании, внедрении, сопровождении бизнес приложений на всех его этапах жизненного цикла. В качестве основных бизнес приложений или функциональных возможностей можно выделить (но не ограничивать) следующие:

- Управление продажами (заказы, счета, платежи, оплаты и т.п.)
- Управление финансами (план счетов, бюджет, расходы, доходы, налоги и т.п.)
- Управление закупками (закупки, контракты, логистика, тендеры, и т.п.)
- Управление складом (поступление, списание, резервы и т.п.)
- Управление персоналом (зарплата, налоги, сотрудники и т.п.)
- Управление производством (ERP)
- Управление рисками и качеством
- Управление инвестициями
- Управление клиентами и Маркетинг (CRM)
- Отчетность и аналитика
- Интеграция бизнес процессов
- Система рассылки сообщений (Web/SMS)
- Системы документа оборота
- Информационный центр
- Информационные Базы и каталоги
- Система управления отелем (Hospitality/Property Management System HMS/PMS)
- Система телевидения и телевидения
- Системы учета и интеграции с телефонией
- Системы управления и интеграции доступом в интернет
- Системы управления продажами (Point of Sales POS)
- Учетные контроля и учета доступа
- Системы онлайн бронирования
- Системы эквайринга
- Системы управления электронными замками

Сайты и публичные ресурсы

Все сайты и внешние системы компании разделяются по категориям:

Информационный сайт (квазистатический). Основная задача сайта – предоставление общей информации о компании/портфеле на всеобщий доступ. Информация на сайте обновляется редко вручную или по средствам панели администрирования.

Информационный сайт (динамический). Задача сайта – предоставление общей информации о компании/портфеле на всеобщий доступ, информация по продуктам, решениям, вопросы-ответы и т.п. Информация на сайте обновляется часто и по средствам загрузки из информационной системы портфеля/компании расположенном в дата центре. Загрузка информации с сайта в информационную систему портфеля/компании происходит не напрямую.

Информационный сайт (интерактивный). Задача сайта – предоставления специфического сервиса компании/портфелю на всеобщий доступ (интернет банкинг, интерактивная поддержка пользователей, интегрирован в бизнес процессы и т.п.) Информация на сайте обновляется часто и по средствам загрузки/выгрузки из информационной системы портфеля/компании расположенном в дата центре. Загрузка/выгрузка информации в информационную систему портфеля/компании происходит напрямую по средствам интеграции систем.

В соответствии с категорией сайта к нему применяются различные требования по внедрению, сопровождению и т.п.

Общие положения для хостинга:

- Сайты должны соответствовать требованиям информационной безопасности
- Сайты размещаются на хостинге в облаке (public cloud web service (SaaS) или private cloud (IaaS))
- Для «динамических» и «интерактивных» сайтов порядок размещения определяется в индивидуальном порядке.
- Размещение сайтов на хостинг в «облаке» позволяет решить вопросы масштабируемости, отказоустойчивости и безопасности, и снижение расходов.
- Администрирование сайтов может вестись самостоятельно ИТ департаментами портфелей, внешними компаниями или же ИТ департаментом компании.

В зависимости от требований организации «облачные» решения могут сократить расходы на ИТ инфраструктуру. Для небольших организаций, или организаций, чья структура географически разбросана, перенос ИТ инфраструктуры полностью или ключевых сервисов, может предоставить огромные преимущества в плане мобильности, безопасности и гибкости, при не значительных расходах.

Системы Информационной Безопасности

Как видно из иллюстрации, в отдельные группы выделены такие технические системы как Системы Информационной Безопасности, Резервного Копирования и Архивирования. Выделение их в отдельные группы связано со спецификой задач и организации предприятия. Так Системы Информационной Безопасности должны покрывать все уровни и компоненты ИТ инфраструктуры и кроме этого могут быть частично или полностью управляется департаментом Безопасности.

Системы Резервного копирования и Архивирования

Тоже самое можно отнести и к системам Резервного копирования и Архивирования. По умолчанию внедрение и сопровождение данных систем является задачами ИТ департамента, и как правило он же является владельцем и управляющим. Для крупной организации или при особых требованиях, функции владения и управления данными системами может быть распределено между департаментами организации.

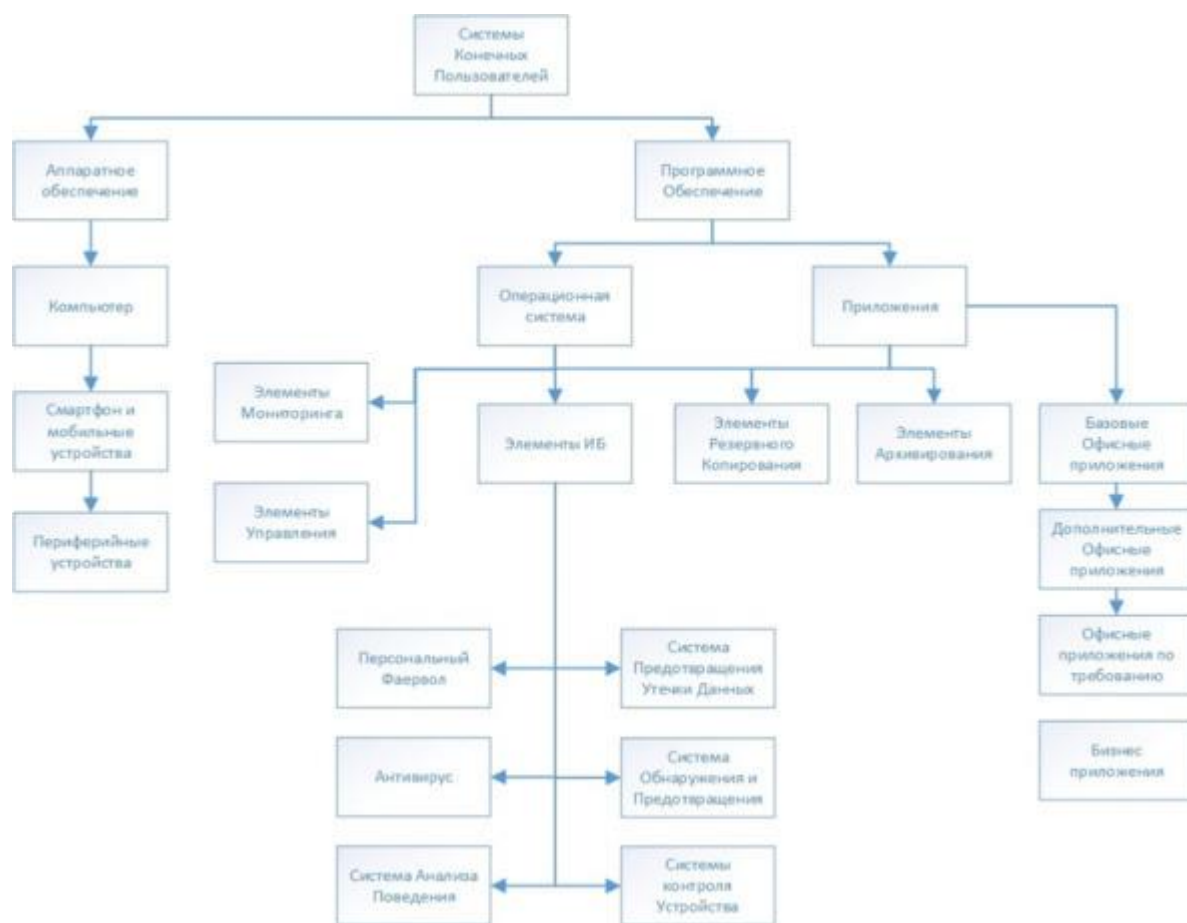
Системы конечных пользователей

Последняя группа – системы конечных пользователей. Данная группа включает в себя решения, призванные обеспечить выполнение функциональных задач сотрудниками при взаимодействии с информационными ресурсами. Как пример – устройства доступа и ввода/вывода информации, клиентская операционная система, офисные приложения и т.п.

Подразделение Поддержки Пользователей обеспечивает сопровождение пользователей и является первичной точкой контакта. К системам можно отнести следующие элементы:

- Пользовательские устройства
- Клиентские операционные системы
- Базовые приложения (Офисные пакеты и т.п.)
- Специализированные приложения (ERP и т.п.)
- Системы защиты информации конечных пользователей

На иллюстрации представлен развернутый вид компонентов систем конечных пользователей. Две основные составляющие систем – аппаратное и программное обеспечение.



В качестве аппаратного обеспечения могут выступать настольные компьютеры, мобильные устройства, тонкие клиенты, а также периферийное обеспечение, такое как мышка, клавиатура, съемные накопители т.п. В качестве программного обеспечения выделяются следующие две основные группы – операционная система и приложения.

Не все элементы могут быть внедрены или же представлять из себя выделенные решения. Так, например, фаервол может представлять из себя встроенную функцию операционной системы, отдельное приложение или приложение в составе отдельного продукта.

Офисная техника

Офисная техника – группа офисного оборудования. Обычно предназначена для использования сотрудниками, конечными пользователями. Может обслуживаться полностью или частично ИТ департаментом, Администрацией или сторонней компанией. Телефония, в зависимости от реализации, может относиться к офисной технике, инженерным системам или ИТ сервисам. В любом случае необходимо определиться со стратегией применения офисного оборудования, как например использование персональных устройств для руководства, multifunctional устройств для рабочих групп и департаментов. При выборе устройств следует определиться со следующими параметрами:

- Выбор типа устройств,
- Выбор вида подключения,
- Формат печати
- Цветность печати
- Скорость печати
- Объем печати
- Ресурс печати

Объем печати в месяц на устройстве должен соответствовать возможностям оборудования. Имейте в виду, стоимость расходных материалов и бумаги составляет одну из главных статей расходов офиса.

Сервисная модель

Компоненты ИТ инфраструктуры можно также представить в виде модели ИТ сервисов.



В данном разрезе компоненты представлены в виде группы ИТ сервисов:

- Корневые
- Первичные
- Вторичные
- Вспомогательные
- Сервисы Информационной Безопасности
- Бизнес сервисы – решения, требования к которым формирует бизнес, и основное предназначение которых – обеспечение бизнес деятельности организации.

Корневые ИТ Сервисы (Core IT Services)

Корневые ИТ Сервисы (Core IT Services) – Необходимые ИТ сервисы и архитектура, без которых невозможно построение являются ИТ инфраструктуры, ИТ является владельцем и управляющим сервисов. В данную группу могут входить:

- Аппаратное обеспечение
- Платформа виртуализации
- Система Хранения Данных (СХД)
- Сетевая Инфраструктура

Первичные ИТ Сервисы (Primary IT Services)

Первичные ИТ Сервисы (Primary IT Services) – Критичные ИТ сервисы, архитектура и технические решения, как правило являющиеся обязательными при построении ИТ инфраструктуры и без которых невозможно предоставление и сопровождение ИТ сервисов, ИТ является владельцем и управляющим сервисов. В данную группу могут входить:

- Служба активного каталога
- Служба DNS
- Центр сертификации
- Служба DHCP
- Система Управления Базами Данных (СУБД)

Вторичные ИТ Сервисы (Secondary IT Services)

Вторичные ИТ Сервисы (Secondary IT Services) – Важные ИТ сервисы и решения, предоставляющие дополнительные возможности по управлению и сопровождению ИТ сервисов или являющиеся частью активности бизнеса. ИТ является владельцем или управляющим сервисов. В данную группу могут входить:

- Файловый сервер
- Сервер централизованной печати
- Удаленный доступ к корпоративной сети
- Удаленного доступа к приложениям
- Сервер корпоративной почты
- Сервис обмена мгновенными сообщениями
- Корпоративный портал
- Система управления проектами
- Сервисная Шина интеграции данных
- Среда разработки и контроля приложений
- Сервис хостинга и облачные решения

Вспомогательные ИТ Сервисы (Accessory IT Services)

Вспомогательные ИТ Сервисы (Accessory IT Services) – Вспомогательные ИТ сервисы и решения, предоставляющие дополнительные возможности по управлению и сопровождению ИТ сервисов и не являющиеся обязательными при построении ИТ инфраструктуры. ИТ является владельцем или управляющим сервисов. В данную группу входят:

- Система обновления
- Система Управления Платформой Виртуализации
- Система Автоматической Установки
- Система Управления конфигурациями
- Система Резервного копирования
- Система Архивирования данных
- Система Мониторинга ИТ инфраструктуры
- Система Управления ИТ сервисами

Бизнес ориентированные ИТ Сервисы (Business IT Services)

Бизнес ориентированные ИТ Сервисы (Business IT Services) – ИТ сервисы и решения, напрямую направленные на выполнение требований бизнеса. Как правило ИТ является управляющим сервисов.

Сервисы защиты информации (Defense IT Services)

ИТ Сервисы защиты информации (Defense IT Services) – ИТ сервисы и решения, основное назначение которых обеспечение информационной безопасности по управлению и сопровождению ИТ инфраструктуры. ИТ является владельцем или управляющим сервисов. В данную группу входят:

- Система защиты периметра
- Система предоставления доступа в интернет (прокси сервер)
- Система защиты почтовых сообщений
- Системы антивирусной защиты (Windows Defender)
- Системы обнаружения и предотвращения вторжения (IDS/IPS)
- Системы защиты веб ресурсов (WAF)
- Обратный прокси сервер (RAP / WAA)
- Системы сбора и обработки событий SIEM

Сканеры уязвимости
Системы управления Идентификацией
Система управления правами доступов
Система шифрования съемных носителей
Система предотвращения Утечки Данных (DLP)
Выделенная система защиты от DDoS атак
Инфраструктура RADIUS сервера
Система двух факторной Аутентификации (OTP)

Системы конечных пользователей (End-Users IT Services)

Системы конечных пользователей (End-Users IT Services) – ИТ сервисы, решения и приложения, устанавливаемые на системы конечных пользователей. Подразделение Поддержки Пользователей обеспечивает сопровождение пользователей и является первичной точкой контакта. К системам можно отнести следующие элементы:

Пользовательские устройства
Клиентские операционные системы
Базовые приложения (Офисные пакеты и т.п.)
Специализированные приложения (ERP и т.п.)
Системы защиты устройств конечных пользователей

Организационная модель

Еще один вариант группировки компонентов ИТ инфраструктуры можно представить на основе организации ИТ. В данном случае группировка может подразумевать распределение сервисов по подразделениям ИТ:

- Инфраструктура
- Специализированные
- Информационная Безопасность
- Конечные пользователи

Инфраструктурные сервисы – компоненты построения инфраструктуры. Могут включать в себя платформу виртуализации, СХД, Управление конфигурациями, сетевая инфраструктура, системы мониторинга, резервного копирования и т.п.

Сервисы общего назначения – также входят в состав инфраструктуры и представлены такими решениями как активный каталог, почтовые и файловые сервера, и т.п.

Сервисы специализированного назначения – к ним могут относиться бизнес решения, среда разработки, шины интеграции и решения, имеющие специфические требования и задачи.

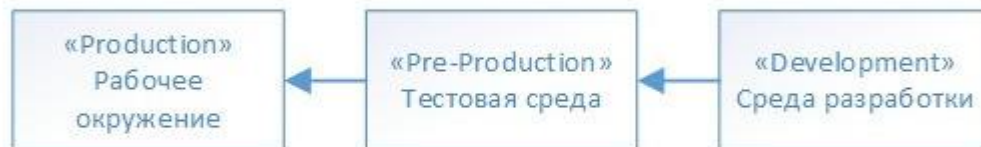
Сервисы Информационной Безопасности – комплексы решения по защите Информации.

Системы конечных пользователей – ИТ сервисы, решения и приложения, устанавливаемые на системы конечных пользователей.

Среда вычислений

Общие Положения

Среда вычислений представляет из себя компоненты ИТ инфраструктуры, сгруппированные по целевому назначению. На иллюстрации можно видеть основные вычислительные среды.



Вычислительную среду «окружение» можно условно разделить на три группы: Рабочее окружение, Тестовая или пред-рабочее окружение и среда разработки.

Среда разработки

Среда разработки (Development) – представляет из себя ИТ инфраструктуру, предназначенную для создания и тестирования новых ИТ сервисов и программных продуктов. Основной упор делается на функционирование самого решения, нагрузочного тестирования, отказоустойчивости и т.п.

Тестовая среда

Тестовая среда (Pre-production) – представляет из себя ИТ инфраструктуру, предназначенную для тестирования новых ИТ сервисов и программных продуктов. Основной упор делается на тестирование решения на взаимодействие с другими ИТ решениями. Подходит для построения концептуальной модели ИТ архитектуры «Proof of concept РОС», эмуляции неисправностей рабочей среды, тестирование изменений и решений и т.п. Как правило представляет из себя «зеркальную» копию конфигурации рабочей среды и частично данных.

Рабочая среда

Среда разработки (Production) – представляет из себя ИТ инфраструктуру, предназначенную для предоставления ИТ сервисов конечным пользователям и заказчикам. Содержит рабочую конфигурацию и данные.

Резервный центр

Последний по списку, но не важности, является вопрос резервирования и в частности наличие резервного центра и уровень его готовности. Данный вопрос относится к теме стратегического планирования и построения ИТ архитектуры. В качестве основных вопросов по созданию резервного центра можно выделить следующие:

- Уровень готовности (резервный, холодный, горячий и т.п.)
- Уровень мощности (полная, частичная от основного сайта, и т.п.)
- Архитектура решения (облако, резервная площадка и т.п.)
- Наличие окружения (рабочая среда, все среды основного и т.п.)

Различают следующие категории специализированных резервных площадок:

- «Горячий» – готовность в течении секунд/минут/часов
- «Теплый» – готовность в течении часов/дней (порядка 48 часов)
- «Холодный» – готовность в течении дней или не полное восстановление
- Не специализированные площадки – использование имеющуюся площади организации (филиал и т п)

В качестве резервной площадки может выступать:

- удаленный офис
- выделенная площадка
- облачная платформа

Как основной подход при построении ИТ архитектуры можно предложить следующие шаги и связки решений:

- Рабочий Центр Обработки Данных ЦОД
- Дублирование и резервирование элементов рабочего ЦОД
- Рабочий ЦОД и внешняя площадка хранения данных
- Рабочий и Резервный ЦОД («холодный»)
- Рабочий и Резервный ЦОД («прогретый» и «горячий»)
- Рабочий ЦОД разнесенный на основную и резервную площадки

Как пример, можно рассмотреть следующие варианты резервного центра:

Отказоустойчивость на уровне резервного сайта («холодного» типа)

Резервные копии серверов сервиса отправляются в резервный центр (автоматически или на съемных носителях). В центре имеются вычислительные ресурсы (физические сервера или платформа) в выключенном или «OFF-LINE» состоянии. Для запуска сервиса необходимо:

- Развернуть необходимое окружение
- Развернуть сервис
- Восстановить резервную копию
- Произвести корректирующие настройки
- Преимущества:
 - Низкая стоимость внедрения
 - Низкая стоимость сопровождения
 - Простота архитектуры

Недостатки:

Время восстановления от 48 часов до нескольких дней

Отказоустойчивость на уровне резервного сайта («теплого» типа)

Резервные копии серверов сервиса отправляются в резервный центр (автоматически). В центре имеются вычислительные ресурсы, развернутые сервера (физические сервера или платформа) в выключенном или «OFF-LINE» состоянии. Для запуска сервиса необходимо:

- Включить по необходимости необходимое окружение
- Восстановить резервную копию
- Произвести корректирующие настройки

Преимущества:

Низкая стоимость внедрения

Время восстановления от 24 часов до 48 часов

Недостатки:

Более высокая стоимость сопровождения

Требует более сложную архитектуру

Отказоустойчивость на уровне резервного сайта («горячий» типа)

«реплики» серверов сервиса отправляются в резервный центр (автоматически). В центре имеются вычислительные ресурсы, развернутые сервера (физические сервера или платформа) в активном состоянии с последними обновлениями конфигурации. Для запуска сервиса может потребоваться произвести корректирующие настройки.

Преимущества – низкая стоимость внедрения и время восстановления от «нулевого простоя» до 24 часов. К недостаткам можно отнести – высокая стоимость внедрения и сопровождения т. к. требует такую же архитектуру, как и для «теплого» типа.

Последовательность внедрения

Последовательность планирования, внедрения и сопровождения ИТ инфраструктуры может включать в себя следующие шаги:

Формирование ИТ стратегии (тип, платформа и т.п.)

Формирование высокоуровневой модели ИТ архитектуры

Подготовка детальной ИТ архитектуры

Расчет требуемых мощностей ИТ сервисов

Расчет платформ вычислений, СХД и коммуникации

Расчет стоимости ИТ сервисов

Формирование требований к инженерным системам

Согласование ИТ архитектуры

Формирование модели организации ИТ

Разработка плана развёртывания

Разработка плана внедрения

Формирования перечня руководящих документов ИТ

При планировании, развёртывании и сопровождении ИТ сервиса старайтесь рассматривать вопросы, указанные на иллюстрации, и по возможности придерживайтесь их.



При развёртывании ИТ сервисов, учитывая ограниченность ресурсов, можно воспользоваться практикой – внедрение решений обеспечивает сторонняя компания, а дальнейшая эксплуатация осуществляется силами ИТ департамента.

Заключение

Группировка компонентов по ИТ сервисам может помочь в понимании стоимости сервисов, их важности, последовательности восстановления, взаимодействия, распределении доступов и т.п. Группировка носит условный и не обязательный характер. Кроме этого, сервисы могут быть перераспределены внутри ИТ департамента между подразделениями, для обеспечения необходимого уровня сопровождения.

В зависимости от требований бизнеса, уровня зрелости компании и т.п. в организации может использоваться все три окружения или даже больше. Как минимум должно быть не менее двух сред – рабочая и тестовая. Требования к мощности, отказоустойчивости, контролю могут варьироваться от компании к компании. Можно предложить следующие ключевые аспекты и рекомендации, на которые стоит обратить внимание, если специально нет требований специфики бизнеса:

- Мощности тестовой среды 1/4 – 1/8 от рабочей
- Мощность среды разработки порядка 1/10 от рабочей
- Можно использовать ресурсы, выведенные из рабочей среды (например, после трех, четырех лет использования в рабочей среде физический сервер выводится и продолжает свою работу как тестовый сервер)
- Срок службы оборудования тестовой среды или среды разработки может быть дольше чем рабочей среды
- Обеспечить изолирование окружений (передача данных, доступ и т.п.)
- Не требуется обеспечивать отказоустойчивость и резервирование тестовой среды и среды разработки на удаленных площадках
- Минимальные требования по резервированию и архивированию
- Политика предоставления и высвобождения ресурсов,

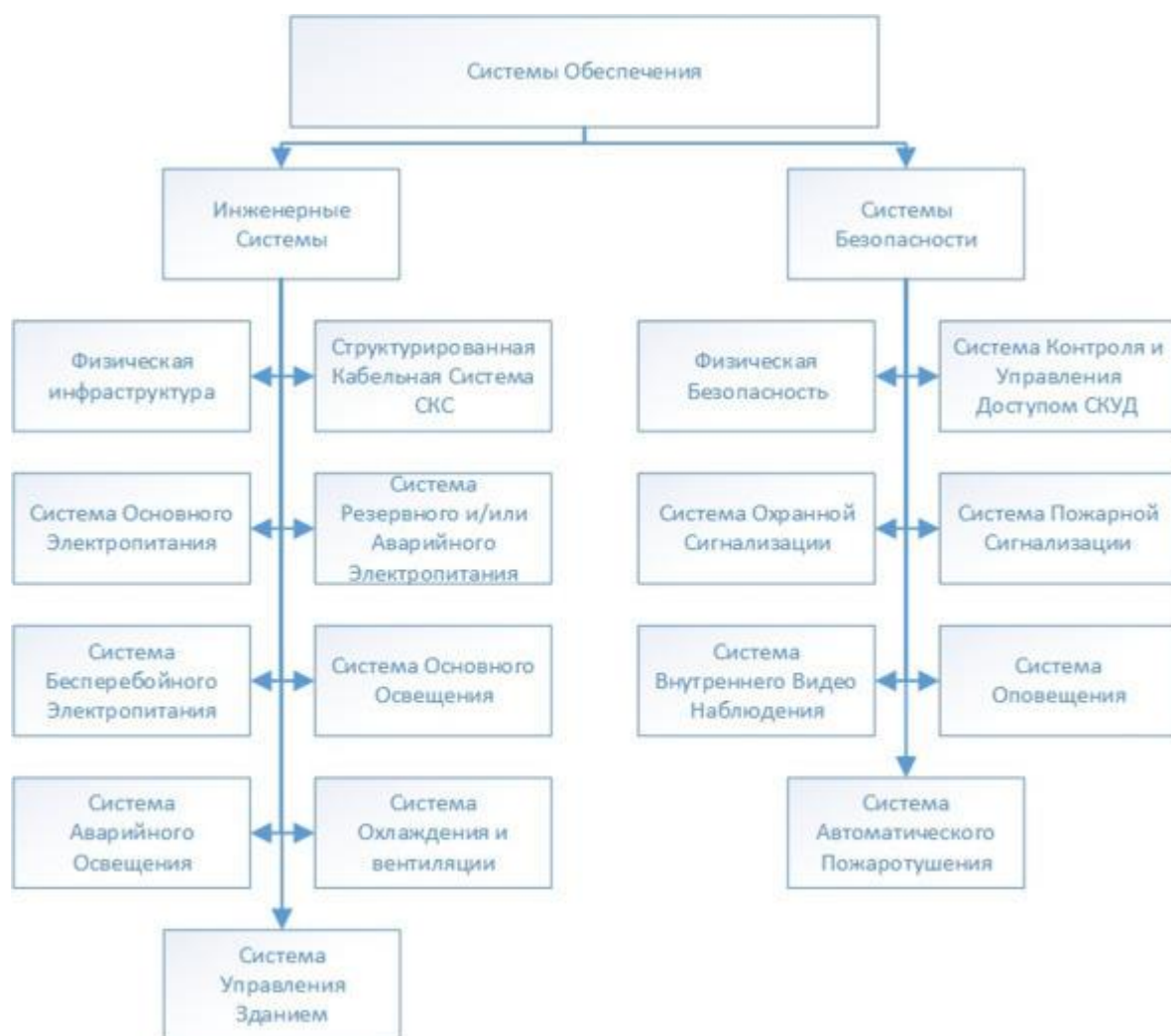
Компоненты Систем Обеспечения ИТ

Общие Положения

Для успешного внедрения и сопровождения ИТ инфраструктуры важную часть играет инфраструктура обеспечения. На иллюстрации представлены составные части инфраструктуры.

В данной главе мы рассмотрим базовые элементы, которые имеют прямое или косвенное отношение к ИТ.

Так система дренажа или котельная может рассматриваться в случаях наличия риска подтопления или пониженных температур.



Системы обеспечения и безопасности ИТ инфраструктуры не являются компонентами ИТ инфраструктуры. Как правило их внедрение и сопровождение производится административным департаментом и департаментом безопасности организации. Но данные системы являются основополагающими для развертывания ИТ инфраструктуры, особенно в случае «on premise» решений.

Понимание основных компонентов, их назначение и возможности может помочь ИТ и организации в целом правильно выстроить ИТ архитектуры предприятия. Введем основные определения:

Дата-центр (Data Center), или центр обработки данных (ЦОД/ЦХОД) – консолидация вычислительных ресурсов и средств хранения данных и связи в специализированном помещении или здании для размещения серверного и сетевого оборудования и выполняет функции обработки, хранения и распространения информации в интересах одного или множества клиентов.

Серверная комната (Server Room) – консолидация вычислительных ресурсов и средств хранения данных и связи в специализированном помещении для размещения серверного и сетевого оборудования и выполняет функции обработки, хранения и распространения информации в интересах данной компании.

Коммуникационная комната – специализированное помещение для размещения элементов СКС, серверного или сетевого оборудования, систем безопасности и т. п. Исполняет функции консолидации, обработки, хранения и обмена информацией с дата-центром компании.

Центр Обработки Данных (ЦОД)

Построение нового ЦОД – это сложный проект, реализация которого невозможна без практического опыта и стратегии развития организации. При проектировании и строительстве вычислительного центра необходимо учитывать множество факторов, часть из которых может быть неочевидной до начала эксплуатации. Процесс построения ЦОД может состоять из этапов:

- Формирование концепции, анализ задач и поиск возможных решений;
- Проектирование ЦОД;
- Строительство ЦОД;
- Ввод объекта в эксплуатацию.

Основной показатель работы ЦОД – отказоустойчивость. Так стандарты Uptime Institute и TIA-942 предполагает четыре уровня надёжности ЦОДа:

TIER I (N) – отказы оборудования или проведение ремонтных работ приводят к остановке работы всего дата центра. В дата центре отсутствуют фальшполы, резервные источники электроснабжения и источники бесперебойного питания, инженерная инфраструктура не зарезервирована;

TIER II (N+1) – имеется небольшой уровень резервирования, в дата-центре имеются фальшполы и резервные источники электроснабжения, однако проведение ремонтных работ также вызывает остановку работы дата-центра;

TIER III (N+1) – имеется возможность проведения ремонтных работ (включая замену компонентов системы, добавление и удаление вышедшего из строя оборудования) без остановки работы дата-центра. Инженерные системы частично (однократно) зарезервированы, имеется несколько каналов распределения электропитания и охлаждения, однако постоянно активен только один из них;

TIER IV (N+N) – имеется возможность проведения любых работ без остановки работы дата-центра. Инженерные системы полностью дублированы и т. п.

Стандарты, регламенты и нормы

В ряде стран имеются стандарты на оборудование помещений дата-центров, позволяющие объективно оценить способность дата-центра обеспечить тот или иной уровень сервиса. Каждый из стандартов, как правило имеет свою внутреннюю классификацию дата центров по совокупности их параметров, и охватывает одну или несколько инженерных систем.

К наиболее известным стандартам по дата центрам можно отнести следующие:

Uptime Institute (UI)

Организация, разрабатывающая стандарты по требованиям и рекомендациям к инженерным системам дата центров при их проектировании, запуске и сопровождении. Вводится понятия уровня TIER дата центра. На данный момент является наиболее полным, структурированным и широко известным. Отличие стандартов Uptime Institute от TIA-942 и других помимо его гибкости заключается также в том, что в них излагаются требования не только технического, но и организационно-управленческого характера. В 2010 году были опубликованы рекомендации Tier Standard: Operational Sustainability. Надёжность и самодостаточность складываются из следующих составляющих:

- надёжность места (оценивается по множеству параметров: от транспортной доступности до степени риска природных и техногенных катастроф);
- надёжность здания (соответствие техническим требованиям, устойчивость к природным и техногенным воздействиям и прочее);
- соответствие назначению (использование надёжных и проверенных технологий, наличие систем резервирования и прочее);

- отдача от капиталовложений;
- управление и функционирование (особенности организации работы, квалификация персонала и прочее).

Американский стандарт (ANSI) TIA-942

В США принят американский стандарт (ANSI) TIA-942, несущий в себе рекомендации по созданию дата центров. В стандарте TIA более подробно расписаны инженерно-технические требования к инфраструктуре дата-центров; имеется в нём и своего рода аналог системы уровней Tier, принятый в Uptime Institute. По сравнению с Uptime Institute менее гибкий.

ASHRAE 90.4 – ASHRAE (Американская Ассоциация инженеров по отоплению, охлаждению и кондиционированию воздуха)

ASHRAE 90.4 – ASHRAE (Американская Ассоциация инженеров по отоплению, охлаждению и кондиционированию воздуха) опубликовала финальную версию стандарта для дата-центров с учетом признания того факта, что уникальные характеристики каждого ЦОДа не позволяют оценивать их по всем тем же стандартам, каким они могли соответствовать до сих пор. Новый стандарт не использует PUE для измерения эффективности дата центра и полностью заменяет PUE двумя более точными метриками: компонент механической нагрузки (КМН, Mechanical Load Component, MLC) и компонент электрических потерь (КЭП, Electrical Loss Component, ELC). В конечном счете эти показатели вошли в финальный вариант стандарта.

Стандарт BICSI 002 2010 (Data Center Design and Implementation Best Practices)

Стандарт BICSI 002 2010 (Data Center Design and Implementation Best Practices), разработанный Международной консультативной службой строительной отрасли (Building Industry Consulting Service International) который дополняет существующие стандарты TIA (TIA-EIA-569-A/B и TIA-942), CENELEC и ISO/IEC, ASHRAE и т.п. По содержанию он во многом близок к TIA-942, но уровни доступности заменены классами. В нём гораздо более детально по сравнению с другими стандартами расписаны технические требования, но при этом нет никакой системы рейтингов и уровней (хотя в одном из разделов перечисляются уровни доступности системы электроснабжения). Обновленная и дополненная версия этого стандарта – ANSI/BICSI 002—2014.

Серия стандартов EN50600 компании «CENELEC»

Серия стандартов EN50600 компании «CENELEC» определяет минимальные требования для инфраструктуры дата центров всех форм и размеров. Они включают в себя защиту от природных катаклизмов, падений и несанкционированного доступа, включая внутренние и внешние экологические события. В стандарте EN 50600-3-1 рассматриваются измерения, контроль и учет энергопотребления в определенных локациях. При правильном применении этого стандарта он может помочь оценить работу дата центра, используя разделы из серии стандартов EN 50600—4 и его ключевые показатели эффективности (Key Performance Indicators KPI). Стандарт EN 50600—4 напрямую управляет факторами эффективности, такими как PUE и REF.

Европейские стандарты ETSI

ETSI ES 205200 определяет так называемые Global KPIs (Глобальные ключевые показатели эффективности), обеспечивая контроль энерго-управления информационно коммуникационных технологий (ИКТ). Этот стандарт предлагает единый глобальный KPI – энергетическое управление обработки данных и коммуникаций – , который определяет четыре целевых KPI: потребление энергии, эффективность выполнения задач, использование возобновляемых источников энергии и повторное использование энергии. Это позволяет определять энергетическую эффективность ИКТ всего предприятия.

Международные стандарты DIS ISO/IEC 30134

DIS ISO/IEC 30134, описывающие KPI дата центра, и отражают стандарты JTC 1/SC 39 WG 1 – новая работа от CENELEC. Во избежание дублирования документов рассматривается их включение в Европейский набор стандартов. Международная электротехническая комиссия IEC

также рассматривает разработку технического отчета, который бы содержал рекомендации по проектированию дата центров применительно к управлению ресурсами.

Стандарт энергетического управления ISO 50001:2011

Стандарт энергетического управления ISO 50001:2011 предоставляет организациям концепцию для интеграции энерго-эффективности в процесс управления. Среди прочего, он включает в себя установку базовых линий, которые измеряются, контролируются и корректируются для обеспечения контроля управления, используя эти данные в качестве базы для текущего прогнозирования, улучшения операций по энерго-эффективности, приобретения и повсеместного размещения эффективного низкоэнергетического оборудования.

Стандарт экологического управления ISO 14001:2004

Стандарт экологического управления ISO 14001:2004 предлагает концепцию обеспечения тщательного контроля интерфейса, чтобы избежать или минимизировать какой-либо негативный экологический эффект. По стандарту ISO 14001 требуется инициативное управление экологическими рисками для поддержки долгосрочных экологических и экономических целей. Следующая редакция – ISO 14001:2015.

Стандарты ITU-TL.1300 от «ITU-T Study Group 5»

ITU-TL.1300 от «ITU-T Study Group 5» в значительной степени основан на инициативе ЕС по уменьшению воздействия на ЦОДы (EU CoC Best Practices V4.0.5) и включает 23 дополнительных пункта. Различия касаются, в частности, предпочтением «ITU-T» ссылаться на диапазон изменения окружающей среды, поддержанный серией стандартов ETSI EN 300 019, нежели на диапазон, указанный в документе Евросоюза.

Стандарты TÜV Süd

Немецкая экспертная организация, один из лидеров в области экспертизы, испытаний и сертификации. Аббревиатура TÜV («Technische Überwachungs-Verein») в переводе с немецкого означает «Объединение Технического надзора». Как одно из направлений деятельности организации разработка стандартов и сертификации дата-центров в Германии.

ГОСТы серии 34

ГОСТ 34. xxx (Единый комплекс стандартов и руководящих документов на автоматизированные системы, ЕКС АС) – комплекс государственных стандартов СССР, межотраслевых руководящих документов и методических материалов, задуманный в конце 80х годов.

Вопросы, связанные с Дата центрами

Положения стандартов UI, BCSI, TIA/EIA—942, EN 50173—5 и ISO/IEC 24764 во многом похожи, однако имеются и различия.

Наличие возможности экстренного отключения нагрузки (англ. Emergency Power-Off, сокращённо ЕРО) является одной из наиболее обсуждаемых проблем, связанных с проектированием и строительством дата-центрах. В разных стандартах она трактуется по-разному.

Согласно стандартам Uptime Institute, возможность экстренного отключения питания в дата-центре не рекомендуется, и нужна лишь в случаях, когда это предписано в местных законодательных актах. Это связано с тем, что экстренное отключение питания нередко становится причиной Даун таймов (например, если кто-то активирует соответствующую функцию по ошибке или невнимательности).

В стандарте TIA-942-2 прямо указано: «Не устанавливать кнопку экстренного отключения питания, если этого не требуют местные власти».

В стандарте BCSI отмечено, что возможность экстренного отключения питания в дата-центре влечёт за собой огромные риски, но в то же время не содержит никаких прямых указаний и рекомендаций; указано, что функция экстренного отключения питания может быть реализована по усмотрению владельцев дата-центра.

Наряду с уровнем доступности и надёжностью важной характеристикой современного дата-центра является энерго-эффективность. Исследованиями эффективного использования ресурсов дата-центрами занимается консорциум Green Grid. Коэффициент энергоэффективности (PUE) вычисляется как отношение общий объём потребляемой энергии (Total Facility Energy) на объём энергии потребляемый ИТ-инфраструктурой (IT Equipment Energy).

Кроме этого в последнее время появляется довольно публикаций по вопросам экологичности эксплуатации дата центров.

Системы обеспечения можно условно разделить на две подгруппы: Инженерные системы и Системы Безопасности.

Инженерные системы

К данной категории можно отнести следующие решения и системы:

Физическая инфраструктура
Структурированная Кабельная Система (СКС)
Система Основного Электропитания
Система Резервного / Аварийного Электропитания
Система Бесперебойного Электропитания
Система Основного Освещения
Система Аварийного Освещения
Система Охлаждения и Вентиляции
Система Управления Зданием

Инженерная инфраструктура составляет большую часть стоимости ЦОД, и нередко достигает до 70%. Распределение затрат на подсистемы дата центров неравномерны. Наибольшая доля, около трети всех потраченных финансовых ресурсов, приходится на стоимость системы гарантированного электропитания (34%). Также значительные траты предусматривают организация кондиционирования (21%) и архитектура самого здания (23%). На коммуникационные сети приходится 7% плюс еще около 9% на оборудование газового пожаротушения, систем управления доступом и видеонаблюдения. Кроме этого имеет значение уровень отказоустойчивости ЦОД.

Стоимость инженерных систем обеспечения ЦОДа может варьироваться в широких пределах и часто зависит от уровня отказоустойчивости. Расчетные расходы можно принять как 22,000—35,000 долларов на 1 м² для дата-центра уровня TIER III, а для уровня TIER IV достигать до 45,000—65,000 долларов на 1 м². В среднем, для дата-центра TIER II+ колеблется в пределах 12,000—33,000 долларов на 1 м².

Физическая инфраструктура

Физическая инфраструктура представляет из себя помещение, здание или пространство для расположения инженерных систем и вычислительных ресурсов. По стандартам построения ЦОД различают помещения ЦОД по их назначению:

- Машинный зал,
- Помещения для коммуникации
- Технические помещения для ИБП и т.п.

Кроме этого вводятся понятия:

- Площадь Стойки (Rack Area)
- Количество Вмещаемых Стоек (Rack Yield)
- Единица Эквивалента Стойки (REU)

По размерам ЦОДы можно разделить по размеру площади серверного зала (машинного зала) и ассоциируется с количеством вмещаемых стоек. Так для примера:

Размер дата центра	Количество стоек	Размер серверного зала
Мини	1-10	До 25 м2 (250 ф2)
Малый	11-200	26-500 м2 (251-5,000 ф2)
Средний	201-800	501-2,000 м2 (5,001-20,000 ф2)
Крупный	801-3,000	2,001-7,500 м2 (20,001-75,000 ф2)

Кроме этого физическая инфраструктура должна предусматривать возможность установки коммутационных комнат и узлов распределения, прокладку кабеля между ними. Для помещений предоставлять возможность установки точек подключения. При ведении проекта необходимо наличия:

- План здания и расположением шахт
- Общий план инженерных систем

Необходимо определить:

- Количество, расположение и размер помещения ЦОД
- Количество, расположение и размер помещений коммутационных помещений
- Количество и расположение отдельно расположенных коммутационных шкафов
- Количество, расположение и размер шахт и их назначение
- Количество, расположение и размер технических помещений

Структурированная Кабельная Система (СКС)

При проектировании СКС здания или дата центра необходимо руководствоваться, но не ограничиваться требованиями общих стандартов TIA-EIA-569-A и TIA-942, а также стандартами СКС:

- EIA/TIA-568C Commercial Building Telecommunications Wiring Standard – американский стандарт;
- ISO/IEC IS 11801—2002 Information Technology. Generic cabling for customer premises – международный стандарт;
- CENELEC EN 50173 Information Technology. Generic cabling systems – европейский стандарт.

Структурированная Кабельная Система (СКС) представляет из себя набор пассивных компонентов компьютерной сети. В качестве элементов СКС можно выделить следующие:

- Коммуникационные шкафы
- Патч-панели – Панели для терминирования кабеля в шкафах
- Кабель
- Кабельные органайзеры
- Кабелеводы, короба для прокладки кабеля
- Модули и розетки рабочих точек
- Коннекторы (RJ-45) кабеля, в случае прямого включения устройств, таких, например, как IP камеры
- Пач-корды для подключения рабочих точек и розеток, активного оборудования и патч-панелей или активного оборудования между собой

Условно СКС можно разделить на две составляющие:

- *вертикальная* – обеспечивает коммуникацию между этажами, отдельными объектами, центрами распределения, коммуникационными стойками и шкафами.
- *горизонтальная* – обеспечивает коммуникацию рабочих точек.

Горизонтальная составляющая СКС включает в себя:

- Центры распределения – узлы агрегирования кабеля.
- Рабочие точки – места подключения конечного оборудования.

Рабочие точки могут представлять из себя набор розеток для подключения конечного оборудования. Например, одна рабочая точка может включать в себя одну розетку ИБП и одну розетку RJ-45.

По возможности всегда обеспечивайте избыточность рабочих точек, как правило порядка 30 процентов и более. Гораздо проще и дешевле обеспечить их прокладку сейчас, чем после введения здания в эксплуатацию.

Как правило в качестве основной среды передачи данных для вертикальной составляющей используется оптический кабель, а для горизонтальной составляющей – «витая пара».

Кабель «витая пара» представляет из себя проводники скрученные попарно и между собой и различается по категориям, определяющим в основном полосу пропускания сигнала и как следствие скорость передачи данных. На данный момент является основным средством (средой) для построения СКС организации.

В таблице представлены основные типы кабеля «витая пара»

№	Маркировка	Скорость передачи данных
1	UTP, U/UTP	неэкранированный кабель
2	FTP, F/UTP	кабель с общим экраном всех пар
3	STP, SF/UTP	кабель с общим двойным экраном сердечника из алюминиевой фольги + «плётки» из лужённых медных проволок
	FTP, U/FTP	кабель с отдельным экраном каждой пары
	F/FTP	кабель с отдельным экраном каждой пары, а так же общим экраном всех пар из алюминиевой «фольги»
	S/STP, S/FTP	кабель с отдельным экраном каждой пары, а так же общим экраном всех пар из лужённых медных проволок

Кроме этого кабель «витая пара» различается по категориям в соответствии с характеристиками.

Таблица основных значений различных категорий указан в таблице ниже.

№	Категория	Полоса пропускания	Скорость передачи данных
1	Cat 1	0,1 МГц	до 10 Мбит/сек, известный как ТРП - «лапша»
	Cat 2	1 МГц	до 4 Мбит/сек, соединяет телефон с телефонной коробкой
	Cat 3	16 МГц	до 10 Мбит/сек
2	Cat 5	100 МГц	до 100 Мбит/сек
3	Cat 5e	125 МГц	100 Мбит/сек используя 2 пары, и до 1000 Мбит/сек (4 пары)
4	Cat 6	250 МГц	1 Гбит/сек с использованием 4 пар, и до 10 Гбит/сек при длине кабеля не более 55 метров
5	Cat 6a	500 МГц	1 Гбит/сек с использованием 4 пар, и до 10 Гбит/сек при длине кабеля не более 100 метров
6	Cat 7	700 МГц	10 Гбит/сек с использованием 4 пар, до 40 Гбит/сек при длине кабеля не более 55 метров, до 100 Гбит/сек при длине кабеля не более 15 метров,

В качестве разъема «витой пары» используется RJ-45 (8P8C) – восьми-контактный компьютерный разъем как наиболее распространённый.

В качестве разъема оптического кабеля используется LC.

Наиболее часто используемый кабель на данный момент Cat6, который заменил Cat5e, в виду относительно низкой стоимости.

Помимо кабеля «витая пара» в ряде случаев может использоваться оптический или коаксиальный кабель, или беспроводные соединения.

Необходимо соблюдать ограничения среды передачи и протоколов связи:

- витая пара – 100 м (между активными устройствами)
- коаксиальный кабель – до 500 м
- оптический мультимодовый кабель – до 500 м
- оптический одномодовый кабель – до 10 км
- беспроводная среда (ненаправленная антенна при условии прямой видимости) – до 300 м

Относительно скорости передачи данных по СКС можно придерживаться: Для базовых решений:

- От компьютера к коммутатору доступа – 100 Мбит/сек
- От коммутатора доступа к ядру – 1000 Мбит/сек

Для продвинутых решений:

- От компьютера к коммутатору доступа – 1 Гбит/сек
- От коммутатора доступа к ядру – 10 Гбит/сек

При ведении проекта необходимо наличия:

- План здания и расположением шахт
- План помещений здания
- Дизайнерский план помещений (для определения рабочих точек)
- Детальные план инженерных систем

Необходимо определить:

- Количество и расположение шкафов в помещении ЦОД
- Количество и расположение шкафов в коммутационных помещений
- Количество, расположение и размер отдельно расположенных коммутационных шкафов

- Количество, расположение и размер шахт и их назначение
- Количество, расположение и размер технических помещений
- Количество, расположение и тип рабочих точек

Для обеспечения мониторинга СКС на физическом уровне (правильность подключения, отслеживание состояния и т.п.) может применяться специализированное решение (например, AMP TRAC). В этом случае стоимость построения СКС может вырасти на 30%.

Система Основного Электропитания

ЦОДы можно разделить по плотности энергопотребления стоек. Так для примера:

Значение плотности	На стойку	На машинный зал
Низкая	0-4 кВт	0-4 кВт
Средняя	5-8 кВт	5-8 кВт
Высокая	9-15 кВт	9-15 кВт

Плотность стойки для разных этапов вычисляется по-разному:

- для этапа проектирования определяется как максимальная (пиковая) нагрузка в кВт на стойку, а плотность серверного зала является средней пиковой плотностью на стойку по всему серверному залу.
- для этапа эксплуатации определяется как измеряемая средняя нагрузка в кВт на стойку, а плотность серверного зала является средней плотностью на стойку по всему серверному залу.

Некоторое активное ИТ оборудование может потребовать отдельные линии питания. Так коммутаторы ядра или шасси «лезвий» может потребовать источники электропитания от четырех до тридцати кВт.

Система Резервного / Аварийного Электропитания

Система резервного электроснабжения используется при выходе из строя или отключения основной линии электропитания.

Системы аварийного электроснабжения подразумевают включение на случай аварии или выхода из строя основного и резервного источников питания.

В общем случае, генераторы можно принять как систему резервного и аварийного электропитания.

Система Бесперебойного Электропитания

ИБП – Источник Бесперебойного Питания, обеспечивает защиту настольного компьютера, сервера и прочего активного ИТ оборудования от кратковременных сбоев в электроснабжении или на момент переключения с основного электропитания на резервный. Может иметь полное или частичное резервирование.

При определённых условиях может являться долгосрочной резервной системой бесперебойного электропитания, когда нет возможности установки дизель генератора.

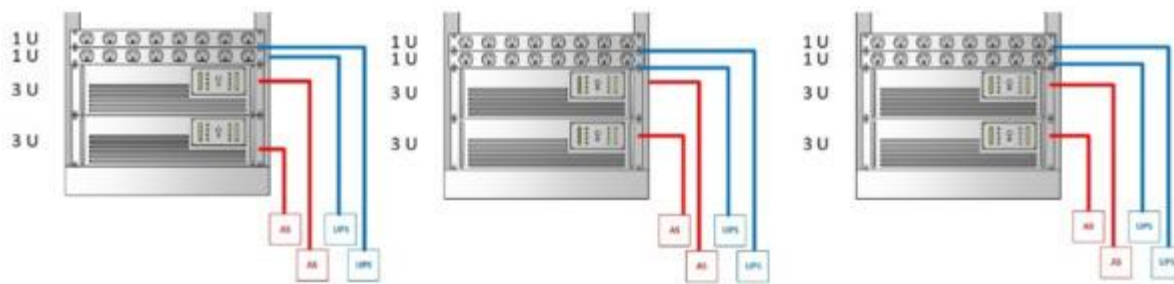


Схема установки и включения источника бесперебойного питания в ЦОД может иметь вид, представленный на диаграмме. В данной реализации, к каждой стойке подводится питание от центрального ИБП (синие линии), а также в каждой стойке локально установлены один или два ИБП в качестве резерва, которые питаются от городского питания. Данная схема достаточно распространена. Если организация следует рекомендациям стандартов и имеет достаточно средств, то желательно не устанавливать резервные ИБП в стойки.

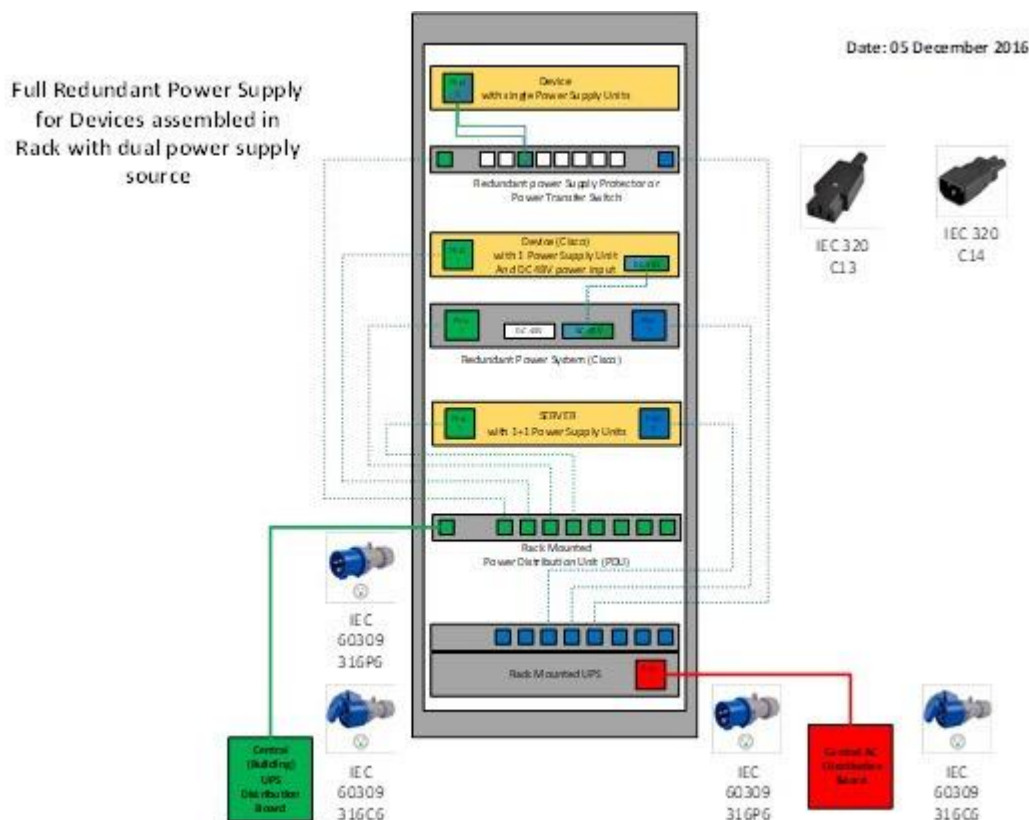


Схема бесперебойного электропитания активного оборудования стойки может иметь следующий вид. Каждое активное оборудование имеет два блока питания (1+1), подключенных к различным источникам бесперебойного питания. Для устройств, имеющих один блок питания можно использовать специализированное оборудование, показанное на схеме. К ним можно отнести Redundant Power Supply (RPS) или Automated Power Switch (APS).

Система Основного Освещения

Со стороны ИТ к системе основного освещения как правило не предъявляются дополнительные требования.

Система Аварийного Освещения

Со стороны ИТ к системе аварийного освещения обычно не предъявляются дополнительные требования. Основное требование, если оно не регламентируется контролирующими органами,

обеспечение минимального освещения в случае аварии, пожара и т. п. Возможно использование двух вариантов:

- Отдельная линия с ИБП с переключением
- Использование светильников с автономными источниками питания

Второй вариант позволяет использовать аварийное совместно с основным. В нормальном режиме светильники питаются от основной линии и резервной линии, как и основное освещение. При сбоях или авариях, при отключении основного электропитания и полном обесточивании, аварийные светильники автоматически переходят на внутренние батареи. Недостатком данного решения может служить относительно высокая стоимость решения.

Примеры комплексной системы электроснабжения

Комплексная система электроснабжения призвана обеспечить защиту оборудования от угроз, представленных на диаграмме.

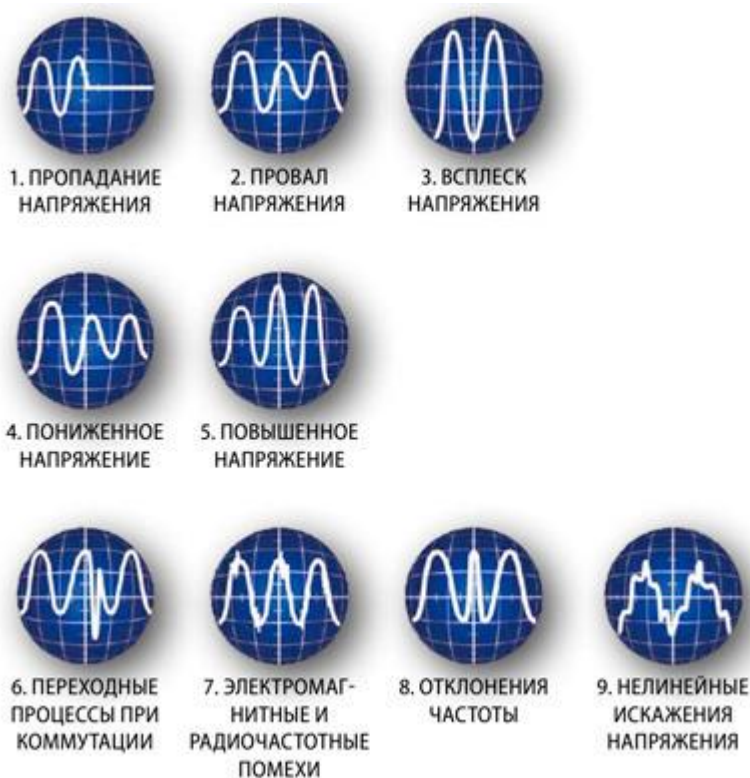


Диаграмма: угрозы электропитания

Схема электроснабжения в комплексе, может включать в себя следующие компоненты и их возможные варианты включения:

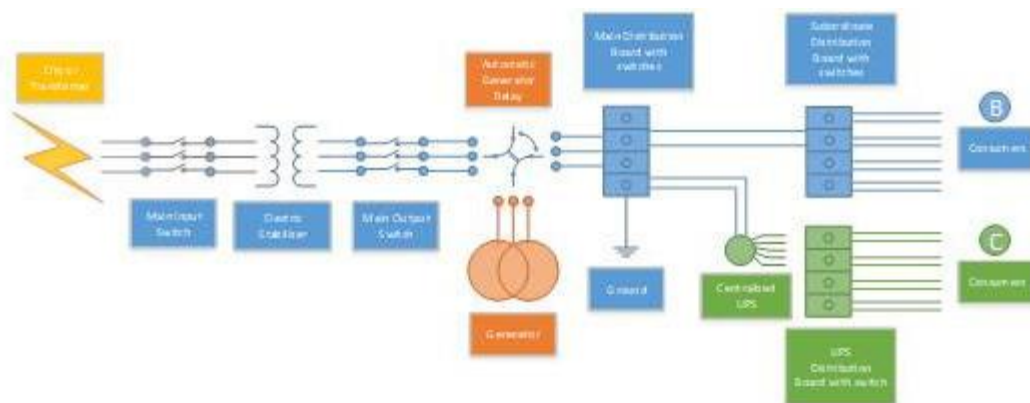


Диаграмма 12.8: Схема включения вариант А

Схема включения вариант А – обеспечивает:

- Стабилизацию напряжения потребителей (В) и (С),
- Защиту входного напряжения автоматики генератора.
- Аварийным или резервным электроснабжением потребителей (В) и (С) от генератора
- Центральный ИБП обеспечен аварийным или резервным электроснабжением от генератора
- Бесперебойным электропитанием потребителей (С)

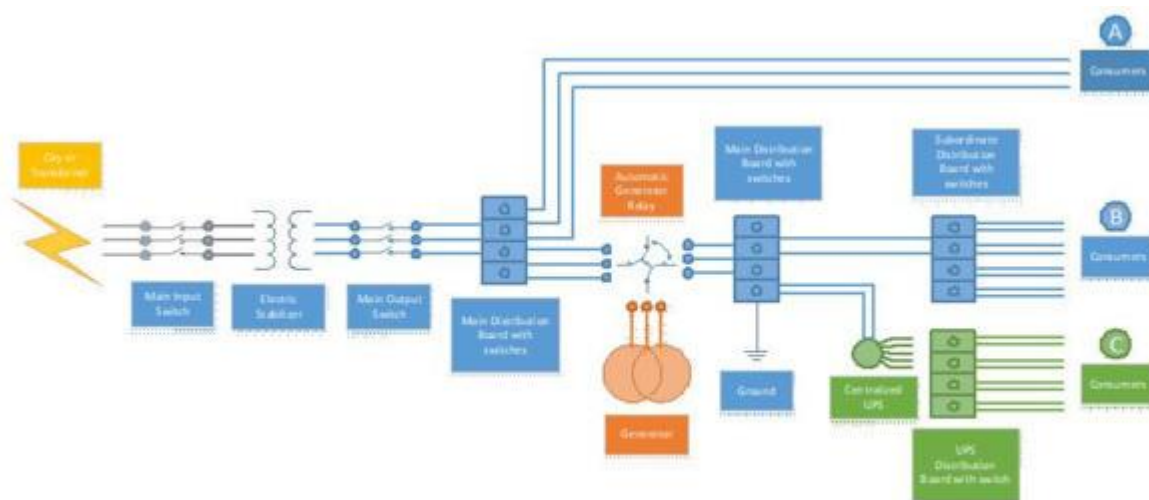


Диаграмма 12.9: Схема включения вариант В

Схема включения вариант В – характеризуется:

- Стабилизацию напряжения потребителей (А), (В) и (С),
- Защита входного напряжения автоматики генератора.
- Не обеспечивает аварийного или резервного электроснабжения от генератора потребителей (А).
- Обеспечение аварийным или резервным электроснабжением от генератора потребителей (В) и (С).
- Центральный ИБП обеспечен аварийным или резервным электроснабжением от генератора
- Обеспечение потребителей (С) бесперебойным напряжением

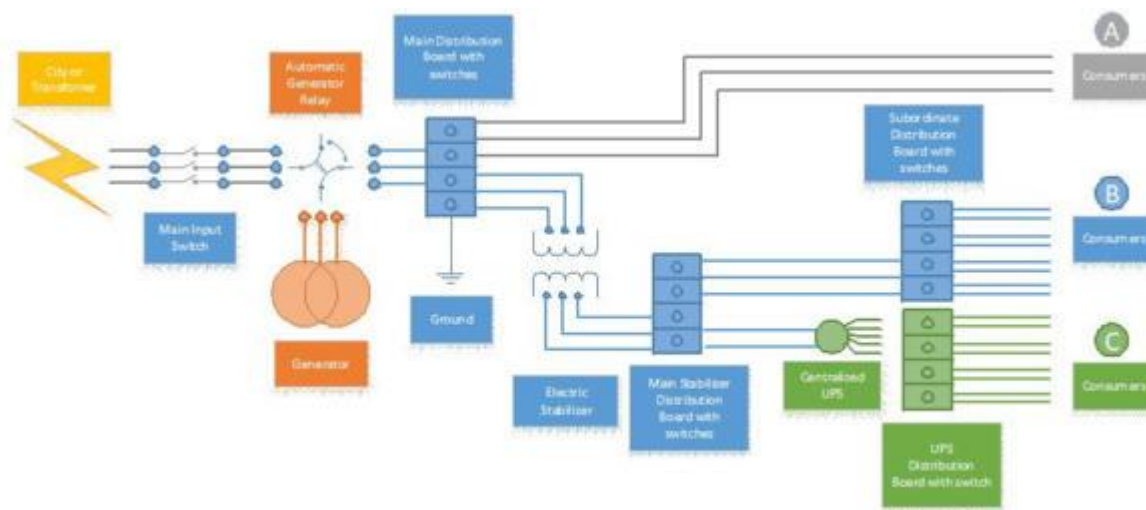


Диаграмма 12.10: Схема включения вариант С

Схема включения вариант С – обладает следующими характеристиками:

- Отсутствие стабилизации напряжения потребителей (А),
- Обеспечение аварийным или резервным электроснабжением от генератора потребителей (А).
- Отсутствие защиты входного напряжения автоматики генератора.
- Обеспечение стабилизации напряжения потребителей (В) и (С),
- Обеспечения аварийным или резервным электроснабжением от генератора потребителей (В) и (С).
- Центральный ИБП обеспечен аварийным или резервным электроснабжением от генератора
- Обеспечение потребителей (С) бесперебойным напряжением

Выбор схемы электроснабжения зависит от требований и финансовых возможностей бизнеса. На схеме показаны участок сети после входного городского электропитания или трансформатора.

Система Охлаждения и Вентиляции

Системы охлаждения могут различаться по следующим характеристикам:

- По типу (естественное охлаждение, классические, сплит, прецизионные или экзотические как «Адиабатическое» охлаждение)
- По элементу охлаждения (газовые или водяные)
- По конструктивным особенностям (напольные, потолочные, настенные)
- По направлению воздушного потока (наддув под фальшпол, прямого надува и т.п.)

При проектировании систем охлаждения необходимо определиться со схемой размещения стоек с активным оборудованием, схемой организации охлаждения и воздушных потоков. В качестве схем охлаждения могут рассматриваться следующие:

- Охлаждение всего помещения
- Схема «Горячего» коридора
- Схема «Холодного» коридора
- Охлаждение стоек

Система охлаждения должна рассчитываться на полную мощность активного оборудования ЦОД. Кроме того, крайне важно иметь резервирование компонентов (N+1, N+M или N+N). Так для примера, при размещении в ЦОД четырех стоек с рабочей нагрузкой порядка 3 кВт на стойку, что составляет порядка 10 кВт максимальной нагрузки, потребует мощность системы охлаждения порядка 40 кВт.

При расчете тепловыделения можно использовать следующие приближенные формулы и особенности использования активного оборудования:

- Мощность резервного блока питания не учитывается
- Мощность тепловыделения устройства принимается как мощность блока питания
- Рабочая мощность тепловыделения устройства принимается как 20—30% мощности блока питания
- Для высоко нагруженных систем можно принимать как 60% мощности блока питания
- Рабочая мощность тепловыделения ИБП принимается как 15% от мощности ИБП (имеется сложная и точная схема расчета)

Система Управления Зданием

Система управления зданием не является обязательным требованием для здания. Система позволяет централизовать и автоматизировать управление системами инженерные здания и обеспечить их взаимодействие. Помимо этого, системы обеспечения могут быть интегрированы с системами безопасности. Владелец системы как правило административный департамент.

Системы Безопасности

К данной категории можно отнести следующие решения и системы:

Физическая Безопасность

Система Управления Контролем Доступа (СКУД)

Система Охранной Сигнализации

Система Пожарной Сигнализации

Система Внутреннего Видео Наблюдения (CCTV)

Система Оповещения

Система Автоматического Пожаротушения

Как правило деятельность по установке и обслуживанию данных систем регламентируется со стороны контролирующих организаций. В организации как правило владельцем и управляющим данных систем является департамент Безопасности.

Физическая Безопасность

Физическая безопасность является комплексом средств и мероприятий по предотвращению несанкционированного доступа к защищаемому объекту. Обеспечивает физическую безопасность как правило департамент Безопасности. Следующие аспекты должны быть приняты во внимание при обеспечении физической безопасности ИТ инфраструктуры:

- Защита помещения ЦОД
- Защита технических помещений систем обеспечения
- Защита помещений коммутационных комнат
- Защита отдельно расположенных коммутационных шкафов

Активное оборудование может иметь степень защищенности, как указан в таблице. Как видно, класс защиты оболочки или оборудования IP (Ingress Protection Rating), например, IP00, IP69 определяет условия эксплуатации оборудования, его стойкость к пыли и влаге.

№	Первая цифра	Вторая цифра
	0 - защиты нет	0 - защиты нет
	1 - защита от твердых частиц размером от 50мм	1 - от вертикально падающих капель
	2 - защита от твердых частиц размером от 12мм	2 - от капель падающих под углом 150
	3- защита от твердых частиц размером от 2,5мм	3 - от капель и брызг падающих под углом 600
	4 - защита от твердых частиц размером от 1мм	4 - от брызг
	5- частичная защита от пыли, защищенная	5 - от водяных струй
	6 - полная защита от пыли, пыленепроницаемый	6 - от мощных водяных струй
		7 - Кратковременное погружение на глубину 1 метр
		8 - Погружение более 1 м до 30 минут
		9 - воздействие с водой высокой температуры

класс защиты оболочки или оборудования IP (Ingress Protection Rating)

Кроме этого, активное оборудование систем безопасности, может иметь степень защищенности, или антивандальный класс, как указан в таблицах. Степень антивандальной защиты IK, например, IK01, IK10, определяет стойкость элементов к ударным нагрузкам.

№	Класс защиты	Масса молотка	Высота падения	Энергия удара
	IK01	0.2 кг	7.5 см	0.15 Дж
	IK02	0.2 кг	10 см	0.20 Дж
	IK03	0.2 кг	17.5 см	0.35 Дж
	IK04	0.2 кг	25 см	0.50 Дж
	IK05	0.2 кг	35 см	0.70 Дж
	IK06	0.5 кг	20 см	1.0 Дж
	IK07	0.5 кг	40 см	2.0 Дж
	IK08	1.7 кг	29.5 см	5.0 Дж
	IK09	5.0 кг	20 см	10.0 Дж
	IK10	5.0 кг	40 см	20.0 Дж

антивандальный класс

Система Управления Контролем Доступа (СКУД)

Система Контроля Доступа не является обязательным требованием для здания (исключение являются специальные объекты), но являются «де-факто» элементом общей системы безопасности. Владелец системы контроля доступа как правило департамент безопасности. Помимо бизнеса рекомендуется обеспечить контроль за доступом к следующим объектам, связанным с ИТ инфраструктурой:

- Помещения ЦОД
- Технические помещений систем обеспечения
- Помещений коммутационных комнат
- Помещения ИТ департамента

Система Охранной Сигналикации

Система охранной сигнализации является обязательным требованием для здания, и обычно устанавливается специальными компаниями. Владелец системы как правило департамент безопасности.

Система Пожарной Сигналикации

Система пожарной сигнализации является обязательным требованием для здания, и устанавливается специализированными компаниями. Являются «де-факто» элементом общей системы безопасности. Владелец системы как правило департамент безопасности.

Система Внутреннего Видео Наблюдения (CCTV)

Системы видеонаблюдения предназначены для ведения видеонаблюдения на объекте. Системы различаются по типу:

- Аналоговые и цифровые видеорегистраторы (DVR)
- Видеорегистраторы на базе компьютера
- Сетевые видеорегистраторы (NVR)
- Серверные и специализированные решения

Используемые камеры по типу (Аналоговые, цифровые, IP камеры), монтажу (Внутренние, внешние, потолочные) и типу (Статические, поворотные, технология «Fisheye»)

Среда передачи сигнала (Коаксиальный кабель, витая пара, оптический кабель, беспроводные соединения) и питания (отдельное питание или технология Power over Ethernet PoE).



Диаграмма: Типовая схема цифровой системы видеонаблюдения

Современные системы видеонаблюдения предоставляют возможность вести дневную и ночную съемку, использование тепловизоров и инфракрасной подсветки, хранение записи автономно или передавать несколькими потоками и форматами, настраивать различные режимы записи (постоянная, по расписанию или по движению), записывать звук, устанавливать границы срабатывания и многое другое. Выбор системы зависит от задач и возможностей компании. При проектировании систем видеонаблюдения необходимо ответить на следующие вопросы:

- количество точек наблюдения
- назначение системы
- условия записи
- время хранения записи

Система Оповещения

Система оповещения, не является обязательным требованием для здания, но являются «де-факто» элементом общей системы безопасности, охраны труда и здоровья. Система

позволяет сообщать работникам и посетителям здания важную информацию, информировать о чрезвычайных ситуациях и т. п. Может представлять из себя отдельные технические средства и административные меры. Владелец системы как правило департамент безопасности.

Система Автоматического Пожаротушения

Система автоматического пожаротушения не является обязательным требованием для здания (исключение специальные объекты) и устанавливается специализированными компаниями. Но являются «де-факто» элементом общей системы безопасности. Владелец системы как правило департамент безопасности.

Административные меры

Помимо наличия технических средств по системам обеспечения ИТ не менее важным аспектом является наличие административных мер. Они могут включать в себя, но не ограничиваться такими действиями как:

- Документирование процессов и процедур эксплуатации средств
- Проведение мероприятий по охране труда и здоровья
- Проведение мероприятий по Пожарной Безопасности
- Проведение мероприятий по Правилам Эксплуатации оборудования и офисной техники

Последовательность внедрение

Последовательность планирования, внедрения и сопровождения систем обеспечения может включать в себя следующие шаги:

- Формирование ИТ стратегии (тип, платформа и т. п.)
- Формирование требований к инженерным системам
- Формирование высокоуровневой модели систем обеспечения
- Подготовка детальной архитектуры систем обеспечения
- Расчет требуемых мощностей для ИТ сервисов
- Расчет стоимости систем обеспечения
- Согласование ИТ архитектуры
- Согласование плана развёртывания
- Согласование плана внедрения
- Согласование перечня руководящих документов ИТ

При развёртывании ИТ сервисов, учитывая ограниченность ресурсов, можно воспользоваться практикой – внедрение решений обеспечивает сторонняя компания, а дальнейшая эксплуатация осуществляется силами компании.

Различают несколько этапов проектирования и внедрения систем обеспечения.

Работы проводимые на этапе начала проекта здания:

- Определение стратегии относительно систем обеспечения
- Определение уровня отказоустойчивости.
- Определение расположения коммуникационных комнат.
- Определение расположения коммуникационных шкафов.
- Определение расположения шахт и каналов.
- Определение расположения технических помещений.
- Формирование технических ИТ требований.

Работы проводимые на этапе строительства или ремонта здания:

- Прокладка внешнего кабеля.
- Прокладка внутреннего кабеля.
- Подготовка к установке систем обеспечения.
- Определение дизайнерского плана офиса.
- Корректировка планов.

Работы, проводимые на завершающем этапе строительства здания:

- Установка активного оборудования систем обеспечения.
- Избирательное или полное тестирование систем обеспечения.

- Передача документации
- Проведение обучения сотрудников
- Корректировка систем.
- Сворачивание временных систем
- Определение формата сопровождения

Заключение

К выбору компонентов систем обеспечения важно приступать на самых ранних этапах планирования постройки или ремонта здания. Крайне важно привлечение ИТ специалистов для формирования требований к системам обеспечения и понимания ими основ функционирования решений.

В данной главе описаны только несколько ключевых моментов связанных с проектированием систем обеспечения. Более подробно, требования расписаны во второй книге серии. В любом случае к процессу проектирования и внедрения и возможно последующему сопровождению систем необходимо привлекать компании, обладающие соответствующей экспертизой.

Послесловие

Жду Ваших ответов и отзывов по электронному адресу: Vadim.aldzhanov@gmail.com. или на сайте книг.

Все желающие дополнить данный документ, могут обратиться к автору и предоставить информацию, выразив свое мнение, рекомендации, поделиться собственным опытом и т.п. Автор оставляет за собой право по внесению изменений и дополнений в книгу.

«ИТ Архитектура от А до Я: Теоретические Основы» – первое издание (версия 0.40),

Автор – Вадим Алджанов,

Тип издания – электронная и печатная книга,

Издание 2018 года,

Объем книги – 766 страницы А5.

ISBN

@ Copyrights Vadim Aldzhanov, 2018