

Предисловие

В апреле 1999 года форумом itSMF в Нидерландах было опубликовано первое официальное издание книги «Введение в ИТ Сервис-менеджмент». Она была воспринята членами форума весьма позитивно, и тираж первого издания составил 18000 экземпляров, что превзошло всеобщие ожидания. Эти цифры показывают серьезный интерес к вопросам ITIL и ИТ Сервис-менеджмента.

Интерес к этой книге за последнее время значительно возрос и со стороны других стран. Сейчас, по прошествии почти трех лет, третье международное и полностью исправленное издание находится перед Вами.

Многие из Вас найдут в книге поддержку, необходимую для внедрения подходов ИТ Сервис-менеджмента в своих компаниях. Опыт показывает, что такое внедрение — непростая задача. С одной стороны, это вызвано стремительным развитием бизнеса, а с другой — тем, что организации, внедряющие ИТ Сервис-менеджмент, часто имеют серьезный фокус на оптимизации своих внутренних процессов. Между тем, ИТ Сервис-менеджмент стал необходимым инструментом для поддержки основных бизнес-процессов компаний. Вопросы разработки и эксплуатации систем все больше формируются под влиянием «точки зрения бизнеса». Кроме того, во многих организациях и индустрии в целом общий курс движения был выбран на профессиональное развитие практических методов, и постоянно предъявлялись требования к краткосрочным и долгосрочным показателям надежности, масштабируемости, гибкости и развития понимания между пользователями и организациями.

Работая с книгой, Вы можете получить наилучшие результаты через обсуждение материала вместе с руководителями Ваших отделов разработок и руководством компании, используя их восприятие как руководящую линию при воплощении этого подхода.

Какие методы ИТ Сервис-менеджмента Вы используете — это чрезвычайно важный вопрос, но необходимо постоянно помнить о том, что конечный результат зависит от мотивации персонала. На этом я желаю Вам успешного использования ИТ Сервис-менеджмента в Вашей организации для обеспечения наибольшей эффективности Ваших корпоративных бизнес-процессов.

Ян Ниессен, председатель ITSMF

Предисловие к русскому изданию книги

Высказывая свое мнение об информационных технологиях, многие из руководителей компаний говорят, что это вынужденная необходимость. Не очень оптимистичное отношение. Удивительно? Но, это так.

Причин, по которым руководство остается недовольным качеством корпоративных информационных технологий (ИТ), много. Часть из них находится в области управления проектами внедрения ИТ. Далеко не всегда проекты завершаются в заданный срок и в рамках выделенных бюджетов. Но даже тогда, когда проекты заканчиваются, становятся актуальными ежедневные вопросы, связанные с использованием ИТ, которые во многом формируют мнение о качестве работы ИТ:

- К кому обращаться?
- Сколько времени департамент ИТ будет обрабатывать мой вопрос?
- Планы требуют видоизменения корпоративных информационных систем. Когда это может быть сделано с условием сохранения текущей функциональности и непрерывности работы для обеспечения деятельности компании в настоящий момент?
- Куда уходят ресурсы, направляемые на сопровождение растущих информационных систем? Насколько эффективно они используются?
- Как организовать работу департамента ИТ в преддверии предстоящего роста компании?

И так далее.

Решение вопросов через руководителей — далеко не самый эффективный путь. Необходимо налаживание горизонтальных связей, позволяющих построить взаимодействие сотрудников на всех уровнях. Книга, предлагаемая вашему вниманию, представляет введение в ИТ Сервис-менеджмент, структурированный подход, позволяющий сделать работу департамента ИТ эффективной и рациональной. Этот подход стал стандартом де-факто в мире для формирования ИТ-службы как современного бизнес-подразделения, то есть департамента, постоянно ориентированного на потребности своих пользователей, нацеленного на решение изменяющихся задач при сохранении прозрачности для руководства с точки зрения достигнутого уровня качества и используемых ресурсов. Опыт показывает, что рассматриваемые принципы организации деятельности актуальны как для небольших, так и для крупных компаний и не зависят от того, передается ли сопровождение ИТ на аутсорсинг или организуется внутренними силами. Качественно работающий ИТ-департамент — это задача, ставшая актуальной для многих современных российских компаний.

Со своей стороны я выражаю благодарность представителям организаций, которые приняли активное участие в работе над книгой, являясь одними из первых в России, кто применил принципы ИТ Сервис-менеджмента в своей работе. Их участие выходило за рамки аудита, и они внесли значительный вклад в создание русской версии книги. Среди них департамент ИТ Сбербанка РФ в лице Хлызова А. Г., Левина А. В. и Аксенова В. Ю., дирекция ИТ компании «ВымпелКом» в лице Барина-ва И. И. и руководство ИТ компании «Чупа Чупс Рус» в лице Крачуна Н. В. Кроме того, я хочу выразить признательность моему коллеге по редакторской работе над книгой Григорьеву М. А., и Ле-винсону А. Б., возглавлявшему работу аудиторского коллектива.

Михаил Потоцкий

Ваши комментарии о русском издании книги, пожалуйста, направляйте в редакторский коллектив русского издания по адресу электронной почты: m.pototsky@itexpert.ru

СОДЕРЖАНИЕ

ВЫХОДНЫЕ СВЕДЕНИЯ

ПРЕДИСЛОВИЕ

5

1 ВВЕДЕНИЕ

13

2 ИТ СЕРВИС-МЕНЕДЖМЕНТ- ОБЩАЯ КАРТИНА

15

2.1. Услуги и качество

15

2.1.1. Гарантия качества

17

2.1.2. Организационная зрелость

18

2.2. Организация и ее политика (правила работы)

21

2.2.1 Корпоративная цель организации, ее миссия и правила

21

2.2.2. Горизонт планирования

23

2.2.3. Корпоративная культура

24

2.2.4. Управление Персоналом

24

2.2.5. Управление

Взаимоотношениями

с Заказчиками ИТ услуг

26

2.3. Процессное управление

27

23.1. Процессы

28

23.2. Процессы и организационные подразделения

30

23.3. ИТ Сервис-менеджмент

31

5.2. Цель процесса

62

3 ВВЕДЕНИЕ В ITIL

33

3.1. Общая картина

33

3.2. Организации

35

3.2.1. OGC(CCTA)

35

3.2.2. Форум itSMF

35

3.2.3. Организации EXINu ISEB

36

3.3. Книги библиотеки ITIL

37

3.3.1. Предоставление услуг

38

3.3.2. Поддержка услуг

40

3.3.3. Другие рассматриваемые процессы

42

4 УПРАВЛЕНИЕ

ИНЦИДЕНТАМИ

47

4.1. Введение

47

4.3.3. Управление Проблемами

52

4.3.4. Управление Изменениями

52

4.3.5. Управление Уровнем Услуг

52

4.3.6. Управление Доступностью

52

4.3.7. Управление Мощностями

53

4.4. Виды деятельности

54

4.4.1. Прием и регистрация

54

4.4.2. Классификация

55

4.4.3. Привязка (сопоставление)

56

4.4.4. Расследование и диагностика

56

4.4.5. Решение и восстановление

56

4.4.6. Заккрытие

56

4.4.7. Мониторинг хода решения

и отслеживание

57

4.5. Контроль процесса

57

4.5.1. Критические факторы успеха

4.5.2. Показатели эффективности

58

4.5.3. Функции и роли

58

4.6 Затраты и проблемы

59

4.6.1. Затраты

59

4.6.2. Проблемы

59

5 УПРАВЛЕНИЕ ПРОБЛЕМАМИ

61

5.1. Введение

5.1.1. Определение — «проблема» и «известная ошибка»

61

5.1.2. Взаимоотношения с Процессом Управления Инцидентами

61

5.3. Процесс

63

5.3.1. Управление Инцидентами

64

5.3.2. Управление Изменениями

64

5.3.3. Управление Конфигурациями

64

5.3-4. Управление Доступностью

65

5.3-5. Управление Мощностями

65

5.3-6. Управление Уровнем Услуг

65

5.4. Виды деятельности

65

5.4.1. Контроль Проблем

65

5.4.2. Контроль Ошибок

67

5.4.3. Проактивное Управление Проблемами

69

5.5. Управление процессом

70

5.5.1. Отчеты об Управлении и Ключевые показатели

4.1.1. Терминология	47	эффективности	70
4.2. Цель	50	5.5-2. Критические	
4.2.1 Преимущества использования процесса	50	факторы успеха	70
4.3 Процесс	51	5.5.3. Функции и роли	71
4.3.1. Входы процесса	52	5.6. Затраты и проблемы	71
4.3.2. Управление Конфигурациями	52	5.6.1. Затраты	71
		5.6.2. Проблемы	72
УПРАВЛЕНИЕ		73.9. Виды деятельности в рамках	
КОНФИГУРАЦИЯМИ	73	Процесса Управления	
Введение	73	Изменениями	98
6.1.1. Основные понятия	74	7.4. Виды деятельности	99
Цель процесса	75	7.4.1. Регистрация	99
6.2.1. Преимущества использования процесса	75	7.4.2. Прием в обработку	100
6.3 Процесс	77	7.4.3. Классификация	100
Управление Инцидентами	77	7.4.4. Планирование	102
Управление Проблемами	77	7.4.5. Координация	103
Управление Изменениями	77	7.4.6. Оценка	105
Управление Релизами	77	7.4.7. Проведение срочных изменений	105
Управление Уровнем Услуг	77	7.5 Контроль процесса	106
Управление Финансами	78	7.5.1. Отчеты для руководства	106
Управление Доступностью	78	7.6 Затраты и проблемы	106
Управление Непрерывностью ИТ-услуг	78	7.6.1. Затраты	106
6.3-9. Управление Мощностями	78	7.6.2. Проблемы	107
6.3.10. Виды деятельности	78	7.6.3. Предложения	107
6.4 Виды деятельности	79	8 УПРАВЛЕНИЕ РЕЛИЗАМИ	109
Планирование	79	8.1. Введение	109
Идентификация	79	8.1.1. Основные понятия	109
Мониторинг статуса	86	8.2 Цель процесса	113
Контроль	87	8.2.1. Преимущества использования процесса	113
Верификация и аудит	88	8.3. Процесс	114
6.5 Контроль процесса	89	8.3.1 .Управление Конфигурациями	115
Отчеты и Ключевые показатели эффективности	89	8.3.2. Управление Изменениями	115
Критические факторы успеха	89	8.3.3 .Управление Уровнем Услуг	115
6.5.3. Функции и роли	89	8.3.4. Виды деятельности	115
6.6 Затраты и проблемы	90	8.4. Виды деятельности	116
Затраты	90	8.4.1. Выработка политики в отношении релизов	
Проблемы	90	8.4.2. Проектирование, компоновка и конфигурирование	116
и планирование	116	8.4.3. Тестирование и приемка релиза	118
7 УПРАВЛЕНИЕ			
ИЗМЕНЕНИЯМИ	93		
7.1. Введение	93		
7.1.1. Основные термины	94		

7.2. Цель процесса	95	8.4.4. Планирование внедрения	118
7.2.1. Преимущества использования процесса	95	8.4.5. Оповещение, и обучение	119
7.3. Процесс	96	8.4.6. Распространение релизов и инсталляция	119
7.3.1. Управление Инцидентами	96	8.5. Затраты и проблемы	119
Управление Конфигурациями	97	8.5.1. Затраты	119
Управление Проблемами	97	8.5.2. Проблемы	120
Управление Релизами	97	9 СЛУЖБА SERVICE DESK	121
Управление Уровнем Сервиса	97	9.1. Введение	121
Управление Доступностью	97	9.2. Цель	122
Управление Мощностями	97	9.3. Структура	122
Управление Непрерывностью ИТ-услуг	98	9.3.1. Доступность	122
13.4.5 Организация процесса и планирование внедрения	177	14.5.2. Критические факторы у^ли и ключевые показатели эффективности	194
Применение превентивных мер и способов восстановления	177	14.5.3. Функции и роли	194
Разработка планов и процедур восстановления	178	14.6. Проблемы и затраты	194
Начальное тестирование	179	14.6.1. Проблемы	194
Обучение и осведомление	179	14.6.2. Затраты	195
13.4.10. Анализ и аудит	179	15 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	197
13.4.11. Тестирование	179	15.1. Введение	197
Управление Изменениями	179	15.1.1. Основные понятия	197
Обеспечение гарантий	179	15.2. Цели процесса	198
13.5. Управление Процессом	9	15.2.1. Преимущества использования	
13-5.1. Отчеты для руководства	179	15.3. Процесс	199
13.5.2. Критические факторы успеха и ключевые показатели процесса качества	180	15.3.1. Взаимоотношения с другими процессами	200
13.5.3. Функции и роли	180	15.3.2. Раздел по Безопасности Соглашения об Уровне Сервиса	204
13.6. Проблемы и затраты	180	15.3.3. Раздел по Безопасности Операционного Соглашения об Уровне Услуг (OLA)	205
Затраты	180	15.4. Виды деятельности	205
Проблемы	181	15-4.1. Контроль — политика и организация информационной безопасности	205
4 УПРАВЛЕНИЕ ДОСТУПНОСТЬЮ	183	15.4.2. Планирование	206
Введение	183	15.4.3. Реализация	207
14.1.2. Основные понятия	183	15.4.4. Оценка	208
Цели процесса	184	15.4.5. Поддержка	208
14.2.1. Преимущества использования процесса	185		
Процесс	186		
Виды деятельности	187		
Определение требований к доступности сервиса	187		

Проектирование систем, для достижения требуемого Уровня Доступности	188
Проектирование систем, для достижения требуемого Уровня Обслуживания	188
Ключевые вопросы безопасности	188
Управление Обслуживанием	189
Проведение измерений и составление отчетов	189
Разработка Плана Обеспечения Доступности	190
Инструментальные средства	191
14.4.9. Методы и методики	191
14.5 Контроль процесса	193
14.5.1. Составление отчетов	193
A.5. Управление Релизами	216
A.6. Управление Доступностью	217
A.7. Управление Мощностями	218
A.8. Управление Непрерывностью ИТ-сервиса	219
A.9. Управление Финансами	220
A.10. Управление Уровнем Услуг	221

ПРИЛОЖЕНИЕ В

В. 1. Акронимы	222
Дополнительный материал	224
Адреса веб-сайтов	225

15.4.6. Составление отчетов	208
15.5. Контроль процесса	209
15.5.1. Критические факторы, у спеха и ключевые показатели эффективности	209
15.5-2. Функции и роли	209
15.6. Проблемы и затраты	210
15.6.1. Проблемы	210
15.6.2. Затраты	210

ПРИЛОЖЕНИЕ А

Фирма «Quick Couriers» («Быстрые курьеры»)	210
A.1. Управление Конфигурациями	212
A.2. Управление Инцидентами и Служба Service Desk	213
A.3. Управление Проблемами	214
A.4. Управление Изменениями	215

Глава 1

Введение

За последние десятилетия информационные технологии (ИТ) оказали большое влияние на бизнес-процессы. Появление персональных компьютеров, локальных сетей, технологии клиент-сервер и Интернета позволило организациям быстрее выводить на рынок свои продукты и услуги. Данные разработки возвестили о переходе от промышленного века к веку информации. В информационном веке все происходит намного динамичнее. В рамках традиционных иерархических организаций часто бывает трудно реагировать на условия быстроменяющихся рынков и это привело к появлению более гибких компаний с меньшей степенью иерархичности. В самих организациях основной акцент сместился от вертикальных функций или отделов к горизонтальным процессам, которые работают в рамках всей организации, а право принятия решения все больше переходит на более низкие уровни. На таком фоне развивались Процессы Управления ИТ-услугами.

В 80-х годах качество ИТ-услуг, предоставляемых британскому правительству, было таким, что существовавшее в то время Центральное агентство по вычислительной технике и телекоммуникациям (Central Computer and Telecommunications Agency — ССТА, в настоящее время именуемое Office of Government Commerce — OGC) получило указание разработать принципы эффективного и рентабельного использования ИТ-ресурсов в министерствах и других государственных учреждениях Великобритании. Целью данной кампании была разработка единого подхода, не зависящего от поставщика услуг. Результатом усилий явилась **Библиотека передового опыта организации ИТ (IT Infrastructure Library — ITIL¹)** которая выросла из собрания лучших методов, существовавших в индустрии ИТ-услуг.

Библиотека ITIL предоставляет подробное описание наиболее важных видов деятельности в работе ИТ, а также полный перечень сфер ответственности, задач, процедур и контрольных списков действий, которые могут быть адаптированы для любой организации. В тех случаях, когда это возможно, виды деятельности определены как процессы, охватывающие сервисные ИТ-службы. Широкая предметная область публикаций ITIL делает полезным регулярное обращение к ним и использование при определении целей для совершенствования ИТ-организаций.

На базе библиотеки ITIL некоторые коммерческие компании разработали свои структурированные подходы к Управлению ИТ-услугами. Среди них HP ITSM Reference Model компании Hewlett-Packard, IT Process Model компании IBM, MOF компании Microsoft и многие другие. Это стало одной из причин, по которым библиотека ITIL фактически стала стандартом в описании фундаментальных процессов ИТ Сервис-менеджмента (IT Service Management — ITSM)². Такое принятие библиотеки ITIL напрямую отражает ее философию и делает ее долгожданной областью знаний, поскольку она послужила толчком к установлению единообразия в индустрии ИТ, столь необходимого в современной распределенной среде.

Более широкое распространение библиотеки ITIL было затруднено отсутствием начальной, но достаточно эффективной книги, являющейся основой для самообучения. Данная книга предназначена для тех, кто участвует в Управлении ИТ-сервисами или интересуется данной темой. Для широкой аудитории в мире дополнительным каналом информации является некоммерческая организация «Форум по ИТ Сервис-менеджменту» (itSMF). Цели, преследуемые itSMF и этой книгой, одинаковы.

«Цель itSMF- как независимой и некоммерческой организации – продвижение современных знаний и опыта в области ИТ Сервис-менеджмента».

Свою миссию itSMF видит в следующем:

itSMF движется к этой цели путем проведения конференций, семинаров, издания журнала, публикации книг. Форум itSMF также заинтересован в привлечении новых членов.

¹ ITIL является зарегистрированной торговой маркой агентства ССТА/OGC

² Термин «ИТ Сервис-менеджмент», с одной стороны, используется как синоним термина «управление ИТ-услугами», но, с другой стороны, усиливает его, имея в виду централизованный подход к менеджменту всей ИТ-организации как современным сервисным подразделением, направленным на предоставление услуг бизнес-подразделениям и являющимся неотъемлемым звеном в производственном процессе. - Прим. ред.

Данная книга, публикуемая itSMF, ставит перед собой следующую цель:

«Сделать знания и опыт по ИТ Сервис-менеджменту доступными для более широкой аудитории»

Итак, задачами книги являются:

1. Содействие миссии itSMF путем публикации доступного руководства по ИТ Сервис-менеджменту, которое также можно использовать при подготовке к сдаче экзаменов по ITIL.
2. Принятие ITIL в качестве фактического стандарта и структурированного подхода¹ для изложения материала книги.
3. Движение вперед и ввод в употребление относительно новых терминов, областей знаний и методов, что сделает область ИТ Сервис-менеджмента более доступной широкой аудитории и разработает общую терминологию для новых публикаций.
4. Гарантия независимости содержания от влияния конкретных поставщиков.

Принимая во внимание быстрое развитие данной области, книги ITIL не всегда могут дать описание самых последних разработок. ITIL, в первую очередь, — собрание передового опыта, накопленного в индустрии, а теория и практика не всегда шагают рядом. При написании книги мы хотели собрать воедино разработки в данной области, не отходя при этом существенно от публикаций ITIL. Поэтому данная книга может быть использована как самоучитель при подготовке к экзамену по ITIL и как введение в более широкую область ИТ Сервис-менеджмента. В этом издании не рассматривается планирование и внедрение ITIL-процессов. Хотя в главе 2 «ИТ Сервис-менеджмент — общая картина» эти вопросы затрагиваются через рассмотрение более широких понятий, таких как качество, процессы и правила работы компании².

Первое издание книги базируется на публикациях itSMF, изданных в Нидерландах, как введение в ИТ Сервис-менеджмент. Эта книга, в свою очередь, основывалась на главах «Краткие сведения для руководства» и некоторых описаниях из официальных изданий библиотеки ITIL с разрешения OGC. Полное издание проверялось многими аудиторами из числа членов itSMF. Детальное последнее редактирование издания книги было выполнено Карен Феррис (Karen Ferris) из компании KMF Advance. Принимая во внимание стремление к единодушию и согласию в области ITIL, мы будем рады новым разработкам, дополнительным материалам и другим творческим вкладам ITIL-профессионалов. Они будут обсуждаться редакторами и, в случае признания подходящими, будут включаться в новые издания.

Ян Ван Бон,
главный редактор
Май, 2002 г.

Пожалуйста, направляйте Ваши комментарии об этом издании в редакторский коллектив книги по адресу: c/o Inform-IT, P.O. Box 23, 9841 PA Grijpskerk, The Netherlands или по адресу электронной почты: jvbon@wxs.nl.

¹ Framework (здесь и далее — англ.).

² Policy (англ.). В данном случае — линии поведения, правила работы компании. Иногда переводится термином «внутренние политики компании».

Глава 2

ИТ Сервис-менеджмент: общая картина

В данной главе рассматриваются такие вопросы как услуги (сервисы), качество, организация, политика компании и Управление Процессами. Эти понятия образуют общий фон для разработки системного подхода к ИТ Сервис-менеджменту.

Процессы Управления ИТ-услугами (также называемые Управлением ИТ), описанные в книге, будут понятны лучше всего на фоне таких концептуальных понятий как организация, качество и услуга (сервис), так как именно эти понятия оказали влияние на развитие ИТ Сервис-менеджмента. Они помогут понять связи между различными элементами библиотеки ITIL. К настоящему времени ITIL — это наиболее известное описание подходов в области ИТ Сервис-менеджмента, и поэтому оно используется в качестве основы для данной книги. В этой главе уделяется внимание следующим понятиям:

- **Услуги и качество:** в разделе рассматриваются вопросы взаимосвязи Уровня Качества с точки зрения его восприятия заказчиками и пользователями, с Управлением Качеством, обеспечиваемым поставщиком (провайдером) ИТ-услуг.
- **Организация и правила работы (policies):** в разделе рассматриваются такие концептуальные понятия как представление компании о своей корпоративной цели (vision), стратегических задачах (objectives) и внутренней политике (правилах работы — policies), обсуждаются вопросы планирования, корпоративной культуры и Управления Персоналом, а также координация бизнес-процессов компании с работой ИТ-служб.
- **Управление Процессами:** в данном разделе рассматриваются вопросы Управления Процессами ИТ Сервис-менеджмента.

2.1. Услуги и качество

Часто организации в значительной степени зависят от ИТ-услуг. Они ожидают, что ИТ-услуги будут не только поддержкой организации, но и дадут новые возможности для реализации целей бизнеса. Более того, ожидания заказчика могут существенно меняться со временем.

Провайдеры ИТ-услуг также уже не могут себе позволить концентрироваться только на технологических аспектах и своих внутренних организационных вопросах. В настоящее время они должны задумываться над качеством предоставляемых услуг и взаимоотношениях со своими заказчиками.

Предоставление ИТ-услуг охватывает все вопросы менеджмента ИТ-инфраструктур, включая обслуживание и сопровождение.

Перед покупкой любого **продукта** в магазине, мы обычно оцениваем его качество по внешнему виду, пригодности и надежности. В магазине у покупателя немного возможностей повлиять на качество продукта из-за того, что он уже произведен на фабрике. Путем тщательного контроля производства изготовитель будет стараться поставлять продукцию с одинаковым Уровнем Качества. В этом примере изготовление, продажа и потребление выступают отдельными друг от друга этапами.

Услуги предоставляются при непосредственном взаимодействии с заказчиком. Качество услуги нельзя оценить заранее, это делается только при ее предоставлении. Качество в определенной степени зависит от того, как поставщик взаимодействует с заказчиком. В отличие от процесса производства, услугу можно изменить на этапе ее предоставления заказчику. Как заказчик воспринимает услугу, и что думает поставщик о том, что он поставляет — все это в значительной степени зависит от их личного опыта и ожиданий.

Процесс предоставления услуги - это сочетание производства и потребления, в котором поставщик и заказчик участвуют одновременно.

Восприятие заказчика является существенным фактором при предоставлении услуг. Обычно заказчики задают себе следующие вопросы при оценке качества услуги:

- Отвечает ли услуга связанным с ней ожиданиям?
- Могу ли я ожидать получение такой же услуги в следующий раз?
- Предоставлена ли услуга по разумной цене?

Насколько услуга отвечает **ожиданиям**, в большей степени зависит от того, насколько хорошо были предварительно согласованы параметры сервиса во время диалога с заказчиком, чем от самого предоставления услуги.

Непрерывный диалог с заказчиком является необходимым условием для усовершенствования услуги и для того, чтобы и заказчик, и поставщик знали, чего стоит ожидать. В ресторане официант вначале расскажет о меню и при подаче нового блюда поинтересуется, все ли нормально. Официант активно координирует спрос и предложение на протяжении всего времени посещения ресторана клиентом, а затем использует полученный опыт для улучшения обслуживания других посетителей.

Качество услуги — это показатель того, насколько услуга отвечает требованиям и ожиданиям заказчика. Для обеспечения качества поставщик должен постоянно оценивать, как услуга воспринимается заказчиком, и что клиент ожидает получить в будущем. Что для одного заказчика является обычным, для другого будет чем-то особенным. И в конечном итоге заказчик может привыкнуть к тому, что в самом начале считалось особенным. Результаты оценки можно использовать для определения того, нужно ли модифицировать услугу, предоставлять ли заказчику больше информации о ней или стоит изменить ее цену.

Качество - это совокупность характеристик продукта или услуги, которые формируют способность продукта удовлетворять сформулированные и подразумеваемые потребности (ISO-8402).

Понятие «**разумная цена**» можно рассматривать как производное понятие. После того, как достигнуто Соглашение об Ожиданиях Заказчика, можно обсудить цену. На данном этапе поставщик должен знать, каковы его затраты на сервисы и какие существуют текущие рыночные расценки на аналогичные услуги.

Заказчик будет недоволен тем поставщиком, который иногда работает выше ожиданий, но разочаровывает в другой раз. Обеспечение **постоянного качества** является одним из наиболее важных, но и наиболее трудных аспектов индустрии услуг.

Например, ресторан должен закупать свежие продукты, поварам нужно работать вместе для достижения хорошего общего результата, и обслуживающий персонал, по возможности, должен иметь одинаковый профессиональный уровень. Ресторану будет присвоено только три звезды, если высокое качество обслуживания будет непостоянным. Ситуация не всегда бывает такой стабильной: обслуживающий персонал может быть разным по своей профессиональной подготовке, хорошее мнение на рынке может поменяться, повара могут уйти и открыть свои рестораны. Обеспечение стабильно высокого качества предполагает скоординированную работу всех элементов: чем лучше и быстрее работает кухня, тем быстрее обслуживаются посетители.

Таким образом, при предоставлении услуг общее качество обслуживания складывается из качества составляющих процессов, которые вместе образуют услугу. Такие составляющие процессы формируют цепочку, звенья которой влияют одно на другое и на качество услуги в целом. Для эффективной координации составляющих процессов требуется не только адекватное качество при выполнении каждого процесса, но еще и качество согласования процессов между собой.

2.1.1. Гарантия качества

Поставка продуктов или услуг требует работы, то есть совершения определенных действий. Качество продукции или услуги во многом зависит от того, как организована работа. Цикл качества Деминга (Deming) (рис. 2.1) представляет собой простую и наглядную модель Управления Качеством. Согласно данной модели, для предоставления соответствующего Уровня Качества нужно непрерывно повторять следующие этапы:

- **Планирование (Plan):** что нужно сделать, когда это нужно сделать, кто должен это сделать, как это следует сделать и с помощью чего.
- **Выполнение (Do):** выполнение запланированных работ.
- **Проверка (Check):** определяется, дал ли выполнение работ ожидаемый результат.
- **Действие (Act):** производится корректировка планов с учетом информации, полученной на этапе проверки.

Для эффективного и своевременного управления необходимо разделение видов деятельности в ходе предоставления услуг на процессы, для которых имеются свои планы и возможности контроля. В организации должно быть четко определено, кто отвечает за данный вид деятельности и кто может изменять планы и процедуры не только для каждого из видов работ, но и для каждого из процессов.

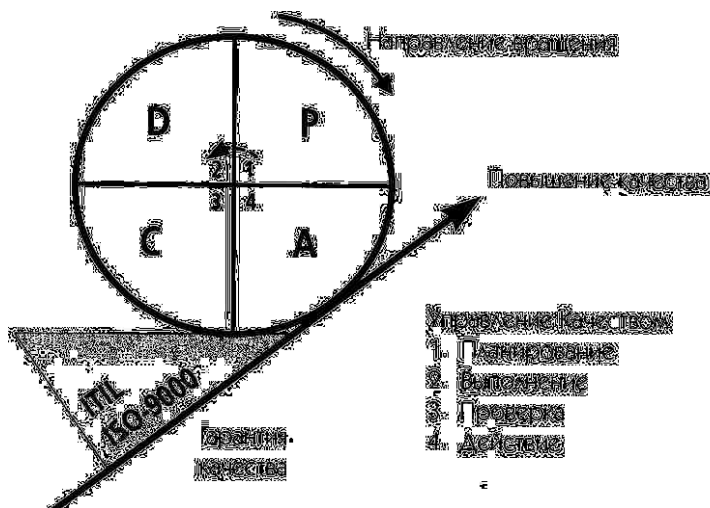


Рис. 2.1. Цикл качества Деминга

Управление Качеством — это обязанность каждого работника организации, предоставляющей услуги. Каждый должен знать, как его вклад в работу организации влияет на качество работы его коллег и, в конечном итоге, на качество услуг, предоставляемых организацией. Управление Качеством также предполагает непрерывный поиск возможностей для совершенствования самой организации и выполнение работ по улучшению качества.

Гарантия качества — вопрос внутренней политики организации. Это совокупность используемых в организации методов и процедур, которые обеспечивают соответствие предоставляемых услуг ожиданиям заказчика и существующим договоренностям. Гарантия качества означает, что улучшения, появившиеся в результате Управления Качеством, поддерживаются постоянно.

Система обеспечения качества — это организационная структура, определяющая распределение обязанностей, используемые процедуры и ресурсы, необходимые для реализации Управления Качеством. Для разработки, оценки и усовершенствования системы обеспечения качества часто используются стандарты серии ISO-9000.

Доктор Эдвард Деминг (Edward Deming) американский статистик, которого компания General Douglas MacArthur направила в Японию после Второй мировой войны для восстановления разрушенной экономики. Он разработал теорию наиболее эффективного использования знаний и творческих возможностей в организациях США в 30-х годах прошлого века, но из-за Великой депрессии его идеи не были реализованы. Однако оптимизационные методы Деминга были успешно использованы в Японии.

Вот некоторые из положений теории Деминга:

- Заказчик является наиболее важной составляющей частью процесса производства.
- Недостаточно удовлетворить заказчика один раз, прибыль приносят заказчики, возвращающиеся к Вам и рекомендующие Вашу продукцию или услуги своим друзьям и знакомым.
- Ключ к достижению качества - уменьшение колебаний качества услуг и продукции
- Разрушайте барьеры между подразделениями.
- Руководитель должен уметь взять на себя ответственность и быть лидером.
- Постоянно совершенствуйтесь.
- Создайте действенную программу обучения и самообучения.
- Организуйте обучение на рабочих местах.
- Преобразование (Transformation) – задача каждого

Стандарт качества ISO-9000:

Некоторые организации требуют от своих поставщиков наличие сертификатов на соответствие стандартам ISO-9001 или 9002 Сертификат служит подтверждением того, что поставщик располагает соответствующей системой качества, эффективность которой регулярно оценивается независимыми аудиторами.

ISO (International Organization for Standardization) это международная организация по стандартизации. Система обеспечения качества, соответствующая стандарту ISO, гарантирует следующее:

- поставщик предпринимает меры по обеспечению качества, согласованного с заказчиками;
- руководство регулярно оценивает работу системы обеспечения качества и, по мере необходимости, использует результаты внутреннего аудита для улучшения ее функционирования;
- процедуры работы поставщика задокументированы и переданы тем лицам, кто зависит от них;
- претензии заказчика регистрируются, рассматриваются в течении разумного срока и, по мере возможности, принимаются во внимание при усовершенствовании услуг;
- поставщик контролирует производственные процессы и может их совершенствовать.

Сертификат ISO не является абсолютной гарантией качества предоставляемых услуг, тем не менее, он служит показателем серьезного отношения поставщика к вопросам обеспечения качества и его готовности обсуждать эти вопросы. Новые стандарты серии ISO-9000 - ISO-9000 – 2000 – по сравнению с предыдущими еще больше внимания уделяют способности организации извлекать уроки из полученного опыта и реализовывать на практике непрерывный процесс улучшения качества.

2.1.2. Организационная зрелость

Опыт работ по улучшению качества ИТ-услуг показал, что недостаточно заниматься только структурированием существующей практики. Причины несоответствия предоставляемых услуг требованиям заказчика часто кроются в способе Управления ИТ-организацией. Для постоянного совершенствования качества требуется определенная степень зрелости организации.

Для определения зрелости организации можно использовать модель, разработанную Европейским фондом Управления Качеством (EFQM — European Foundation for Quality

Management) (рис. 2.2). С помощью данной модели определяются основные сферы деятельности, которые следует принимать во внимание при Управлении Организацией.

Цикл качества Деминга входит составной частью в модель EFQM. Действия (определение стратегии, курса движения организации) предпринимаются на основе результатов, полученных в тех областях, которые предполагают их получение. Такие действия являются фундаментом планирования (например, структуры процессов), целью которого является достижение желаемых результатов. Модель EFQM определяет девять сфер деятельности.

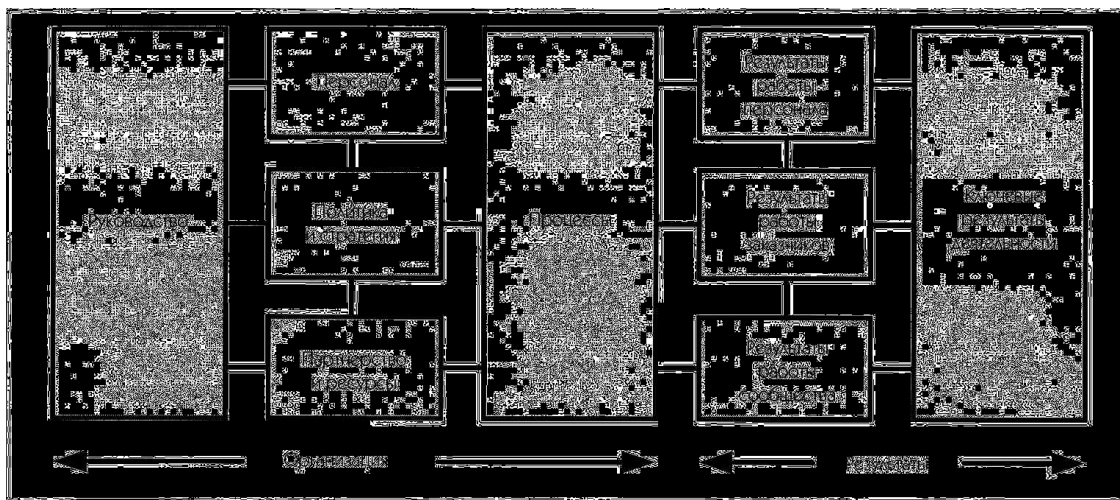


Рис. 2.2. Модель EFQM

Голландская организация по вопросам качества (INK) дополнительно поделила модель EFQM на этапы, давая тем самым возможность определить, в какой степени компании удалось реализовать общее Управление Качеством в отдельной области и в организации в целом. Определено пять этапов:

- **Нацеленность на продукт** — этап, известный как ориентированный на результат; все в организации работают напряженно (но в этих усилиях отсутствует направленность); деятельность организуется специальным образом для каждого конкретного случая.¹
- **Нацеленность на процесс** — этап также известен под названием «мы знаем, что делаем»; деятельность организации имеет плановый и повторяющийся характер.
- **Нацеленность на систему** — или «сотрудничество подразделений».
- **Нацеленность на цепочку**² — этап также известен под названием «внешнее партнерство»; организация концентрирует усилия на том качестве, которое она добавляет как составляющий элемент к цепочке поставщик-заказчик.
- **Нацеленность на всеобщее качество**³ — этап, называемый «рай на земле»; организация достигла такого уровня, когда постоянное и сбалансированное стремление к совершенствованию стало нормой.

Сферы деятельности, определенные с помощью модели EFQM, можно увязывать с показателями организационной зрелости. Уровень Зрелости организации в каждой из этих областей определяется с помощью анкетирования. Такую оценку могут провести собственные или приглашенные аудиторы.

После определения Уровня Зрелости организация может приступить к разработке стратегии совершенствования, которая в дальнейшем будет преобразована в план работы. План, который составляется с учетом модели на один год, определяет, какие аспекты в

¹ Ad hoc.

² Под «цепочкой» понимается цепь создания прибавочной стоимости. — Прим. ред.

³ Total quality

каждой сфере деятельности нужно улучшить и как это сделать. Путем повторения процесса самооценки и планирования организация сможет контролировать Уровень своей Зрелости. Основные преимущества данного подхода следующие: организация может улучшать качество поэтапно; промежуточные результаты становятся наглядными; руководство организации может вести ее по выбранному стратегическому курсу.

В дополнение к подходу EFQM существует много других видов самооценки и проверки организационной зрелости. Некоторые из них сфокусированы в основном на внутренней структуре организации. Следует помнить, что совершенствование отдельных элементов внутренней структуры организации может лишь частично повлиять на общие результаты компании в тех случаях, когда не совершенствуются отношения с заказчиками, персонал не получает удовлетворения от работы, не улучшается руководство организацией или же когда стратегия и тактика организации четко не определены.

В ИТ индустрии процесс развития Уровня Зрелости наиболее известен через Модель зрелости (Capability Maturity Model — CMM). Эта модель была создана в институте разработки программного обеспечения (ПО) (Software Engineering Institute — SEI) в университете Карнеги-Меллона (Carnegie Mellon). Она предназначена для совершенствования процессов разработки ПО и повышения степени зрелости этих процессов. Модель CMM включает в себя следующие уровни:

- **Начальный уровень** — процессы выполняются индивидуально для каждого конкретного случая.¹
- **Уровень Повторяющихся Процессов** — процессы становятся повторяющимися и организованы, таким образом, чтобы качество услуг стало повторяющимся.
- **Уровень Документированных Процессов** — процессы в организации документированы, стандартизованы и интегрированы.
- **Уровень Управляемых Процессов** — организация оценивает полученные результаты и использует их для повышения качества предоставляемых услуг.
- **Уровень Оптимизирующихся Процессов** — организация постоянно оптимизирует свои процессы с целью повышения качества услуг или разработки новой технологии или сервисов.

На основе вышеперечисленных Уровней Зрелости процессов были разработаны модели ИТ Сервис-менеджмента.

Разрабатывая и сопровождая системы качества, отвечающие требованиям стандарта серии ISO-9000 (ISO-9000-2000), организация может достичь Уровня «Нацеленности на систему» (или Уровня «Управляемых процессов» по терминологии модели CMM). Эти стандарты ISO уделяют основное внимание определению, описанию и проектированию процессов.

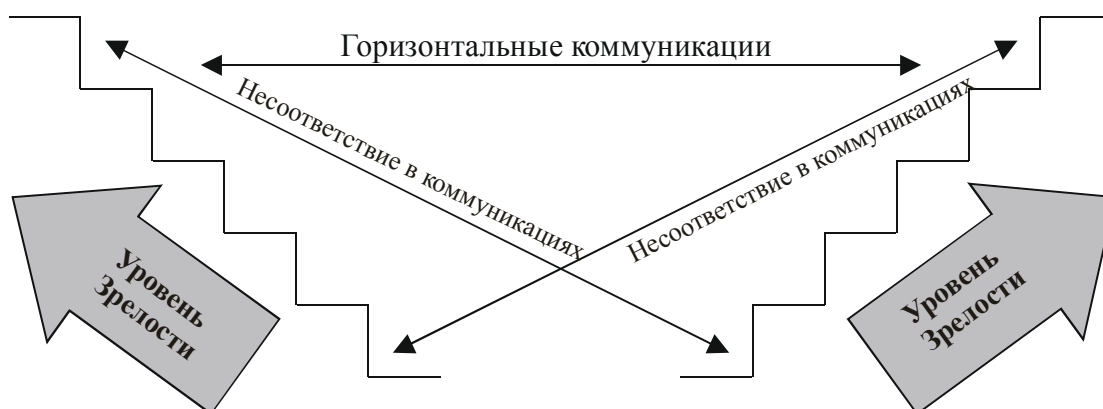


Рис. 2.3. Связи заказчик-поставщик и Уровни Зрелости

При оценке зрелости организации нельзя ограничиться только поставщиком услуг. Здесь также важен Уровень Зрелости Заказчика (рис. 2.3). Если разница в степени зрелости компаний заказчика и поставщика велика, то ее следует учитывать, если нет желания столкнуться с несоответствием

¹ Ad hoc

подходов и стилей работы в этих компаниях. Особенно это относится к организации взаимодействия между заказчиком и поставщиком. Целесообразно, чтобы компании заказчика и поставщика выходили на одинаковый Уровень Организационной Зрелости, и взаимодействие происходило бы на этом Уровне или было скорректировано с учетом более низкого уровня одного из партнеров.

2.2. Организация и ее политика (правила работы)¹

В предыдущих разделах была проиллюстрирована тесная взаимосвязь качества услуг и качества работы самой организации с ее политикой (правилами работы). В данном разделе будут рассмотрены некоторые важные аспекты работы организации и ее политики, имеющие отношение к вопросу Управления Процессами.

2.2.1. Корпоративная цель организации, ее миссия и правила

Организация — это определенная форма сотрудничества людей. Перед любой организацией, будь это дарте-клуб или мультинациональная компания, стоит вопрос: в чем цель объединения в организацию? Такой **корпоративной целью (vision)** может быть, например, Ваше умение делать деньги, продавая персональные компьютеры. Но для того, чтобы организация стала привлекательной для всех заинтересованных сторон² (например, заказчиков, инвесторов, сотрудников компании и т. д.), вы должны уметь рассказать, почему им интересно иметь дело именно с вами. Может быть, вы самый лучший или самый дешевый поставщик или просто весельчак! Для этого вам следует создать привлекательный имидж. Здесь могут быть использованы такие лозунги, как «Давайте сделаем жизнь лучше!» или «Ты не будешь одинок!» и многие другие.

Для того чтобы сообщить всем свою корпоративную цель, компания может представить ее в виде тезиса о своей **миссии (mission)** (рис. 2.4). Миссия — это короткое и четкое описание задач, стоящих перед организацией, и идеалов, в которые она верит.

Стратегические задачи (objectives) — это более подробное описание того, что хочет достичь организация. Хорошо сформулированные стратегические задачи должны обладать пятью основными свойствами (соответствовать принципу SMART): быть конкретными (Specific), поддаваться измерению (Measurable), быть уместными и соответствующими ситуации (Appropriate), быть реалистичными (Realistic) и иметь четкие временные границы (Time-bound).

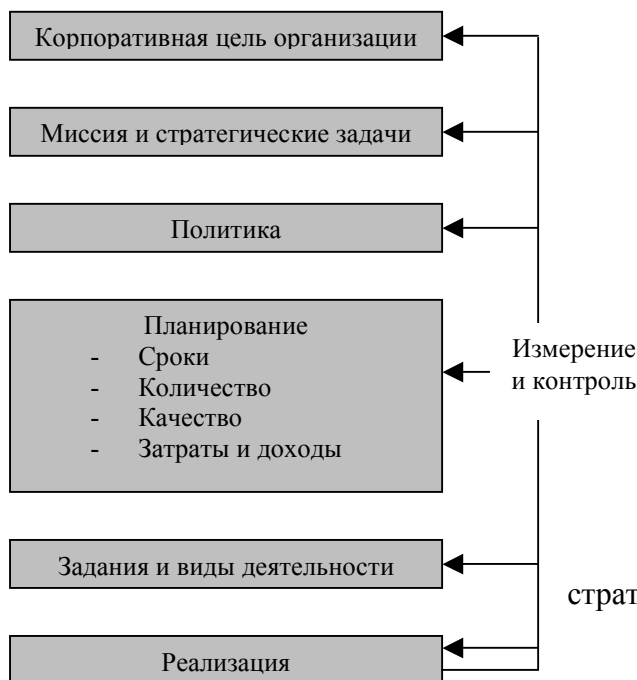


Рис. 2.4. Корпоративная цель организации, ее стратегические задачи и политика (правила работы)

Политика организации (policy) — это совокупность всех решений и мер, принятых организацией для постановки стратегических задач и их достижения. При разработке своей политики организация определяет приоритеты стоящих перед ней

¹ Policies.

² Stakeholders.

стратегических задач и пути их достижения. Безусловно, в зависимости от обстоятельств, приоритеты могут со временем меняться. Чем лучше разъяснена политика организации всем участвующим сторонам, тем меньше возникает проблем при объяснении сотрудникам, как им выполнять работу. В отличие от подробных процедур, эти правила могут быть использованы персоналом организации в качестве руководящих указаний. Четко сформулированная политика (правила) компании способствуют гибкости структуры организации, поскольку все уровни в такой компании могут быстро реагировать на изменение ситуации.

Реализация политики в виде конкретных видов деятельности требует **планирования**. Обычно планы состоят из нескольких этапов, имеющих контрольные точки, в которых выполняется мониторинг хода исполнения работ. Например, на основе политики организации составляется годовой план, который далее используется для разработки бюджетов. Общий план может быть детализирован в планы подразделений на год, квартальные планы или планы проектов. Каждый из этих планов включает в себя определенные элементы: график выполнения работ, требуемые ресурсы, Соглашения о качестве и количестве поставляемых продуктов и услуг.

Для выполнения запланированных работ требуется осуществление определенных **действий**¹. Для персонала действия определяются как **задания**², иногда их выполнение может передаваться сторонним организациям.

Когда на основе миссии организации формируются стратегические задачи, политика, а затем измерять правильность курса организации и, в случае необходимости, проводить его планы и задания, есть риск, что через определенное время миссия, стратегические задачи и правила будут забыты. Для того чтобы этого не случилось, необходимо на каждом этапе корректировку.

Таким образом необходимо измерять, в какой степени организация или процессы близки к достижению своих стратегических целей. Для этого имеются различные методы. Одним из наиболее известных в бизнесе методов является **Карта Сбалансированных Оценок (Balanced Score Card — BSC)**. Согласно данному методу, на основе стратегических целей организации или целей процесса определяются **критические факторы успеха (Critical Success Factor — CSF)**. Такие факторы формулируются для нескольких наиболее важных сфер интересов компании, называемых перспективами (проекциями)³ организации: заказчики/рынок, бизнес-процессы, персонал/инновации и финансы. **Ключевые показатели эффективности (Key Performance Indicators — KPI)** являются теми параметрами, по которым определяется, достигли ли критические факторы успеха (CSF) заданного уровня. При необходимости ключевые показатели эффективности (KPI) могут быть подразделены на показатели эффективности (Performance Indicator — PI).

Ключевые показатели эффективности (KPI) – это параметры, используемые для измерения дохода выполнения работы по отношению к ключевым стратегическим целям организации или критическим факторам успеха (CSF).

Результаты измерений и изменяющиеся обстоятельства могут привести к модификации процессов, задач, планов и политики организации, а также к изменению стратегических задач (objectives), миссии (mission) и корпоративных целей организации (vision). Чем более зрелой является организация, тем легче она справляется с такими изменениями. Если ИТ-подразделение поддерживает интерес бизнеса, то стратегические задачи (objectives) ИТ-подразделения будут определяться стратегическими задачами бизнеса. Например, ИТ-подразделение может иметь стратегическую задачу: «Вносить свой вклад в усиление конкурентоспособности бизнеса». Задания подразделению будут теперь определяться, исходя из этой стратегической задачи. В зависимости от характера бизнеса, стратегические задачи для ИТ-подразделения будут ставиться с учетом надежности, доступности, скорости реагирования, технической сложности ИТ-решений и так далее.

¹ Actions.

² Tasks.

³ Perspectives.

2.2.2. Горизонт планирования¹

Рассматривая политику и планирование работы ИТ-подразделения, необходимо учитывать связь планирования бизнеса в целом с планированием прикладных систем (приложений)² и технической инфраструктуры. При планировании коммуникационных сетей и приложений ИТ-подразделение должно находиться в авангарде общего планирования бизнеса, так как оно обеспечивает создание такой ИТ-инфраструктуры для бизнеса, благодаря которой он сможет развиваться.

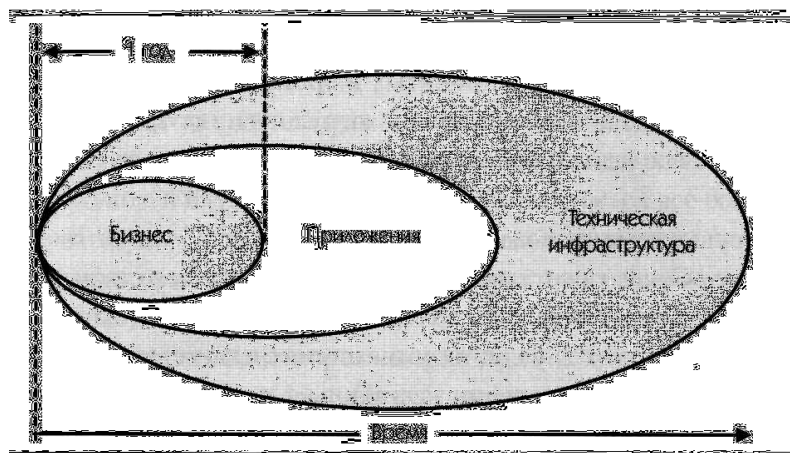


Рис. 2.5. Горизонты планирования

У **технической инфраструктуры** самый дальний горизонт (период) планирования. Она выполняет поддерживающую роль и ее связи с реальной бизнес-деятельностью видны не всегда четко. На разработку инфраструктуры требуется время. Кроме того, зависимость информационных систем и бизнеса от технической инфраструктуры вносит ограничения на проведение ее изменений. Более того, разработка и создание инфраструктуры требует значительных инвестиций, и поэтому следует учитывать период ее амортизации.

У **приложений** горизонт планирования ближе, так как они разрабатываются для выполнения конкретной бизнес-задачи. Планирование жизненного цикла приложения в первую очередь основывается на тех бизнес-функциях, которые должна будет выполнять система, после чего принимаются на рассмотрение технологии, которые могут использоваться для достижения поставленных целей.

Бизнес-планы, составленные на основе стратегии организации, обычно рассчитаны на один календарный или финансовый год. Составление бюджета, планирование, составление отчетов о ходе выполнения работ осуществляется, исходя из этого периода. На некоторых рынках время, отводимое на планирование, еще больше сокращается, как и время для разработки продукта. В планах должны быть отражены четыре аспекта:

- **Время** — самый легкий для определения показатель. Время определяется датой начала и окончания работ, и очень часто разбивается на этапы.
- **Количество** — цели должны поддаваться измерению для осуществления мониторинга хода выполнения. Такие определения целей, как «улучшенный» или «более быстрый», недостаточны для планирования.
- **Качество** — качество результата должно соответствовать поставленной цели.
- **Затраты и доходы** — результаты работы должны быть соразмерны предполагаемым затратам, усилиям и полученным доходам.

Различие в горизонтах планирования наблюдается не только между разными сферами деятельности, но и между разными Уровнями Процессов (стратегическим, тактическим и операционным). Более подробно этот вопрос будет рассматриваться в последующих главах.

¹ Период времени, который требует планирования.

² Applications

2.2.3. Корпоративная культура

Организации, производящие изменения, например ради повышения качества предоставляемых услуг, в конечном итоге столкнутся с вопросами корпоративной культуры, существующей у них в настоящий момент. Под корпоративной (организационной) культурой понимается то, как люди общаются друг с другом в организации, как принимаются и выполняются решения, как сотрудники относятся к работе, заказчикам, поставщикам, руководству и коллегам.

Культуру, которая зависит от норм поведения и ценностей, принятых в организации, нельзя контролировать, но на нее можно влиять. Для оказания такого влияния от руководства требуется демонстрация лидерства, проведение четкой и последовательной политики и поддержка со стороны персонала.

Корпоративная культура может оказать существенное воздействие на оказание ИТ-услуг. Бизнес может относиться к инновациям по-разному. Существуют организации со сложившейся стабильной корпоративной культурой, в которых на инновации не обращают большого внимания. У такой организации могут возникнуть трудности с приведением ИТ-услуг в соответствие с изменениями в организации. С другой стороны, если структура ИТ-подразделения нестабильна и подвержена частым изменениям, то такая корпоративная культура может стать серьезной помехой на пути обеспечения качества услуг. В этом случае может возникнуть ситуация, когда большое количество бесконтрольных изменений приведет к появлению многочисленных сбоев в работе.

2.2.4. Управление Персоналом¹

Политика Управления Персоналом играет важную стратегическую роль в достижении организацией долгосрочных целей (также см. модель EFQM). Она также может быть использована в качестве инструмента изменения корпоративной культуры. Цель современного подхода к Управлению Персоналом — оптимизация производительности работы всего персонала организации. Для этого используются такие средства, как подбор кадров, обучение и продвижение по службе, мотивация труда и вознаграждение (поощрение).

Концепция HRM является основной формой современного Управления Персоналом. Концепция HRM основывается на двух предпосылках:

- Управление Персоналом должно способствовать достижению стратегических целей организации. Если организация должна реагировать лучше и быстрее на еще более быстрые изменения в своем окружении, то это должно найти отражение в подборе и расстановке кадров, качестве и численности персонала.
- Создание работникам организации условий для применения и развития своих способностей и навыков послужит на пользу организации.

Существует три подхода к Управлению Персоналом:

- **Жесткий подход** — в этом случае людские ресурсы рассматриваются как средство производства. Они должны быть организованы наиболее эффективным и рациональным способом (effectively and efficiently). Как и корпоративная стратегия, политика управления персоналом определяется экономическими, техническими и рыночными условиями. При таком подходе значимость работников оценивается по-разному. Некоторые ключевые специалисты стратегически являются более важными, чем другие, вспомогательные работники, которым можно легко найти замену. Например, при таком подходе компания может принять решение, что только ключевые специалисты будут работать на постоянной основе, а все остальные — на контрактной.
- **Мягкий подход** — в этом случае основной акцент делается на наилучшее использование потенциала сотрудников во благо компании. Современные специалисты высокообразованны, честны и готовы многое отдавать работе. Именно поэтому следует как можно раньше определить их потенциал и постоянно развивать его (обучение, создание условий для

¹ Human Resource Management - HRM.

профессионального роста). При определении своей стратегии и политики организация должна опираться на таланты и потенциальные возможности всех своих сотрудников.

- **Интегрированный подход** — такой подход строится на общих интересах персонала и руководства организации. Для достижения целей в организации должен быть нормальный приток, движение и отток кадров. Изменения на рынке и в организации (например, изменение в технологических областях) ведут к постоянным изменениям в спросе на различные специальности.

Все аспекты политики Управления Персоналом должны быть тщательно скоординированы. Перемещение работников в организации, определение и развитие их навыков (компетенции) и содействие мобильности внутреннего рынка труда становятся все более важными для организации. Качество предоставляемых услуг только выиграет от наиболее полного раскрытия потенциала работников организации. Это способствует непрерывному совершенствованию организации. Инструментами улучшения Управления Персоналом являются:

- **Доведение политики организации до ее сотрудников** - объяснение каждому сотруднику, в какой степени его работа способствует достижению целей, стоящих перед организацией. Важным условием успеха в этом направлении является участие в нем всех уровней руководства.

- **Оказание доверия, предоставление полномочий**¹ — сотрудники получают возможность организовывать и выполнять свою работу по согласованию с организацией. Объем предоставляемых полномочий определяет Уровень Ответственности, которую сотрудники несут за качество выполненной работы.

- **Ответственность**² — результат применения двух первых пунктов. Если сотрудникам объяснили, чего от них ожидают, и если они имели возможность организовывать и выполнять свою работу так, как они считали нужным, то они несут полную ответственность за свою работу. Это может служить основой для оценки и вознаграждения сотрудников. Это вознаграждение может быть как материальным, так и нематериальным, например, признание или новые возможности для профессионального роста и развития карьеры и т. д.

- **Управление Уровнем Компетенции**³ — является одновременно как средством наиболее эффективного применения уже имеющихся в распоряжении организации знаний, так и способом систематического развития знаний, необходимых для компании. Данный подход позволяет определять, какой Уровень Компетенции требуется для выполнения необходимых процессов или проектов, а также каким Уровнем Знаний должны обладать сотрудники. При организации работы персонала компания фокусируется не только на достижении нужного баланса между требуемым и существующим Уровнем Компетенции сотрудников, но и на создании условий для развития компетенции, обмена знаниями и обучения новым навыкам. В этом сотрудникам могут помочь наставники⁴. Формирование коллективов сотрудников по областям знаний (по их специализации) способствует обмену опытом и появлению новых областей компетенции.

2 2.2.5. Управление Взаимоотношениями с Заказчиками ИТ-услуг⁵

Качество ИТ-услуг во многом зависит от взаимоотношений с заказчиками. На основе этих отношений разрабатываются и корректируются Соглашения. Сферой действия Управления Отношениями с Заказчиками ИТ-услуг (IT Customer Relationship Management — CRM) является поддержание отношений с заказчиком и координация работы с организацией на стратегическом, тактическом и операционном уровнях. На рис. 2.6 показаны горизонтальные контакты между заказчиками и ИТ-организацией в плане поддержки отношений и координации работы. По вертикали отображены контакты по вопросам политики, контроля и отчетности.

¹ Empowerment — данный английский термин имеет очень широкое значение и подразумевает «усиление» коллектива за счет оказания ему доверия, предоставления дополнительных полномочий, организации доступа к накопленным знаниям и т. д.

² Accountability.

³ Competence management.

⁴ Mentors and coaches.

⁵ IT Customer Relationship Management — IT CRM.



Рис. 2.6. Управление Взаимоотношениями с Заказчиками ИТ-услуг

Основной задачей Управления Взаимоотношениями с Заказчиками ИТ-услуг (CRM) является обеспечение хороших и эффективных связей между ИТ-организацией и организацией заказчика на всех уровнях. Однако на каждом из этих уровней роль CRM будет разной. Одним из элементов взаимоотношений является наличие Службы Service Desk, в то время как контроль над Уровнями Услуг может основываться на Процессе Управления Уровнем Сервиса¹ (SLM). В этих областях Управление Взаимоотношениями с Заказчиками (CRM) играет вспомогательную роль, например, через организацию опросов заказчиков и пользователей, предоставление информации и т. д.

Пользователь - это человек «за компьютером», сотрудник, использующий услуги ИТ для выполнения повседневной работы.

Заказчик - это человек, «платящий по счетам», он имеет полномочия заключать Соглашения с ИТ- организацией на предоставление ИТ- услуг (например, Соглашение об Уровне Услуг – SLA) и отвечает за то, чтобы предоставленные услуги были оплачены.

Очевидно, что «платящий по счетам» заказчик во многих ситуациях может выступать и как пользователь «за компьютером».

Управление Взаимоотношениями с Заказчиками ИТ-услуг играет важную роль в развитии стратегического диалога² между ИТ-организацией и компанией, приобретающей ИТ-услуги. На практике этот вопрос в основном сводится к укреплению контактов с организацией заказчика и использованию возможностей для координации стратегических целей двух компаний. Такой подход может послужить основой для установления долгосрочного сотрудничества, в котором ИТ-организация концентрирует свои усилия на запросах заказчика и предлагает ИТ-решения, позволяющие заказчику достигать свои бизнес-цели. Учитывая динамичный характер как компании заказчика, так и ИТ-организации, степень изменений в обеих компаниях также должна быть скоординирована.

На основе договоренностей с заказчиком о предоставляемых ему услугах посредством Процесса Управления Уровнем Услуг разрабатываются предложения об Уровне Услуг. Например, если заказчик хочет внедрить у себя Интранет, то следует согласовать такие вопросы, как доступность данной

¹ Service Level Management — SLM.

² Используемый здесь английский термин «alignment» дословно переводится как «выравнивание», «согласование», однако по сути отражает необходимость организации диалога между бизнесом и ИТ-департаментом таким образом, чтобы как стратегические, так и важнейшие тактические и оперативные вопросы обсуждались совместно.

услуги, поддержка пользователей, реализация Запросов на Изменения и стоимость. Договоренности по всем этим вопросам ложатся в основу Соглашения об Уровне Услуг (SLA).

Если заказчик хочет изменить (расширить или модифицировать) услуги, оговоренные в SLA, то он подает **Запрос на Изменение**¹ (RFC), который обрабатывается в рамках Процесса Управления Изменениями (Change Management — CHG). Изменения, выходящие за рамки существующих договоренностей, передаются Процессу Управления Уровнем Услуг.

В то же время, в большинстве случаев по рабочим вопросам пользователи могут контактировать со службой **Service Desk**.

Рис. 2.6 дает представление не только о горизонтальных и вертикальных связях, но и о **горизонте планирования** процессов. У согласования на стратегическом уровне горизонт планирования составляет несколько лет. Управление Уровнем Услуг связано с Соглашениями на тактическом уровне, где горизонт планирования равен приблизительно одному году. Управление Изменениями, Управление Инцидентами и Служба Service Desk занимается оперативными вопросами с горизонтом планирования в несколько месяцев, недель, дней или даже часов.

2.3. Процессное управление

Каждая организация нацелена на выполнение своих корпоративных целей и миссии, решение стратегических задач и реализацию выбранной политики. Это достигается через выполнение определенной деятельности. Вспомним наш пример с рестораном, где осуществлялись такие работы, как закупка овощей, ведение бухгалтерского учета, заказ рекламных объявлений, прием гостей, уборка столов, чистка картошки и приготовление кофе.

Имея такой неструктурированный список работ, что-то может выпасть из нашего внимания, и это может привести к ошибке. Поэтому лучше структурировать работы, то есть организовать их таким образом, чтобы было видно, как каждая группа работ способствует решению стратегических задач и как эти группы связаны между собой.

Такие группы организованной между собой деятельности называются процессами. В случае, если процессная структура организации четко определена, то она дает ответы на вопросы:

- Что должно быть сделано.
- Какой ожидается результат.
- Каким образом можно определить (измерить), что в результате работы процесса достигается ожидаемый результат.
- Как результаты выполнения одного процесса влияют на результаты других процессов.

Вопросы, представленные на рис. 2.7 постоянно возникают при использовании процессного подхода, типичного для современного ИТ Сервис-менеджмента. Средства для нахождения ответов на них приведены в правой части рисунка.

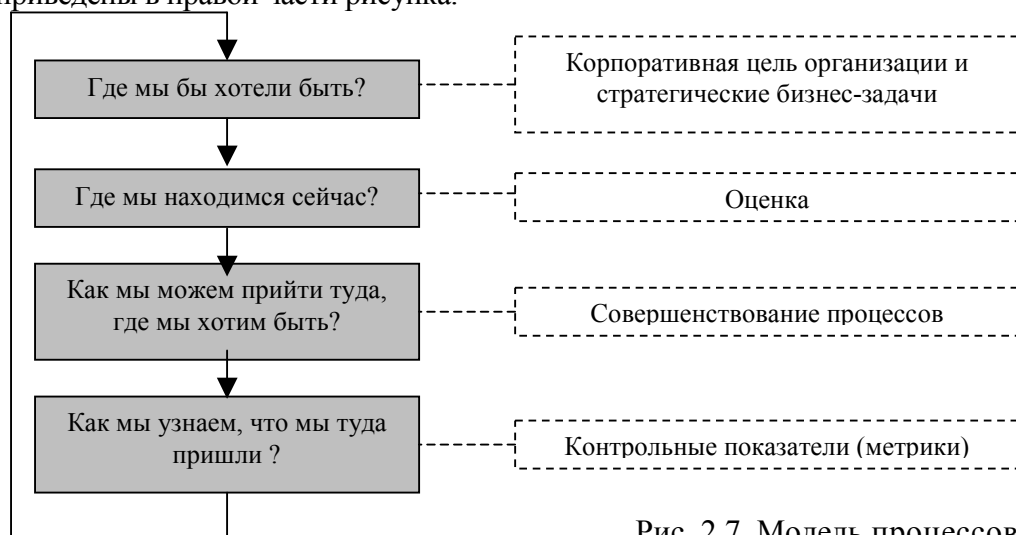


Рис. 2.7. Модель процессов

¹ Request For Change - RFC.

2.3.1. Процессы

При организации работ в виде процессов не учитываются ни существующее распределение работ, ни деление организации на отделы. Это сознательный выбор. Делая выбор в пользу процессной структуры, можно доказать, что некоторые виды работ в организации не координируются, дублируют друг друга, игнорируются или вообще не нужны.

Процесс - это логически взаимосвязанная между собой последовательность работ (видов деятельности (activities)), направленная на достижение поставленной цели.

Вместо этого мы сосредотачиваемся на цели процесса и его взаимоотношениях с другими процессами. Процесс — это последовательность работ, нацеленная на преобразование входных данных (информации, документации и т. д.) в выходные. Для получения информации о том, каким будет результат выполнения процесса, нужно проверить вход и выход каждого процесса на соответствие **характеристикам качества и стандартам**. В результате этого получаются цепочки процессов, по которым можно отследить, что происходит в организации и какой результат получается, а также определить контрольные точки в этих цепочках, в которых выполняется мониторинг качества продуктов и услуг, предоставляемых организацией.

Стандарты для выходных данных каждого процесса должны быть определены таким образом, чтобы вся цепочка процессов обеспечивала достижение корпоративных стратегических целей. Если результат процесса отвечает заданному стандарту, такой процесс будет считаться эффективным (effective). Если работы в рамках данного процесса к тому же выполняются с наименьшими усилиями и затратами, этот процесс будет рациональным (efficient)¹. Цель Управления Процессами — планировать и контролировать процессы таким образом, чтобы они были одновременно эффективными и рациональными.

Для оптимизации качества процессов каждый из них можно рассматривать отдельно. Владелец процесса несет ответственность за результаты работы процесса. **Менеджер процесса** отвечает за его структуру и выполнение и подотчетен владельцу процесса². **Координаторы процесса** отвечают за выполнение заданных видов работ и отчитываются о результатах их выполнения менеджеру процесса.

Логическая структуризация работ внутри процесса позволяет установить четкие точки перехода, в которых есть возможность выполнять мониторинг качества процесса. В примере с рестораном мы можем разделить обязанности по закупке продуктов и приготовлению блюд так, чтобы повара не занимались закупками, и, возможно, не тратили слишком много времени на оценку свежести ингредиентов, которая не влияет на их работу.

Руководство организации может осуществлять контроль, основываясь на информации о качестве каждого из процессов. В большинстве случаев соответствующие показатели эффективности³ и стандарты уже будут predeterminedены Соглашениями. Поэтому каждодневный контроль процесса передается Руководителю (менеджеру) Процесса. Владелец процесса будет оценивать работу по показателям производительности и их соответствию согласованному стандарту. Без четких показателей владельцу процесса будет трудно определить степень контролируемости процесса и реализации запланированных улучшений.

¹ Суть терминов «effective» и «efficient» можно также проиллюстрировать выражениями «делать правильные вещи» и «делать вещи правильно».

² Логическая структуризация работ внутри процесса позволяет установить четкие точки перехода, в которых есть возможность выполнять мониторинг качества процесса. В примере с рестораном мы можем разделить обязанности по закупке продуктов и приготовлению блюд так, чтобы повара не занимались закупками, и, возможно, не тратили слишком много времени на оценку свежести ингредиентов, которая не влияет на их работу.

³ Performance indicators.

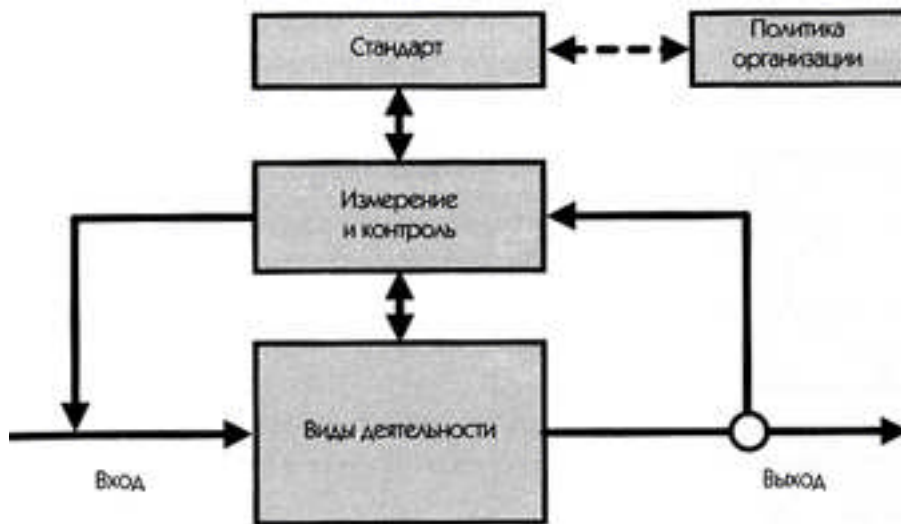


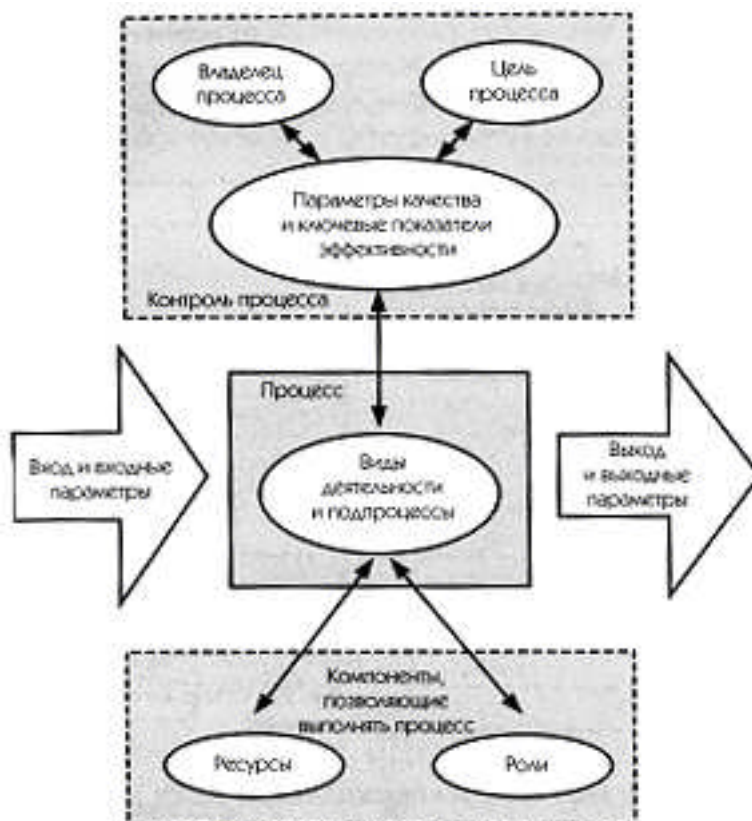
Рис. 2.8. Общая диаграмма процесса

Часто процессы описывают с помощью **процедур** и **рабочих инструкций**.

Процедура – это описание логически связанных видов работ с указанием их исполнителей. Процедура может включать в себя этапы из различных процессов. Процедура определяет, что должно выполняться и кем, и она может меняться в зависимости от организации.

Набор **Рабочих инструкций** определяет, как следует выполнять виды работ, входящие в состав процедур.

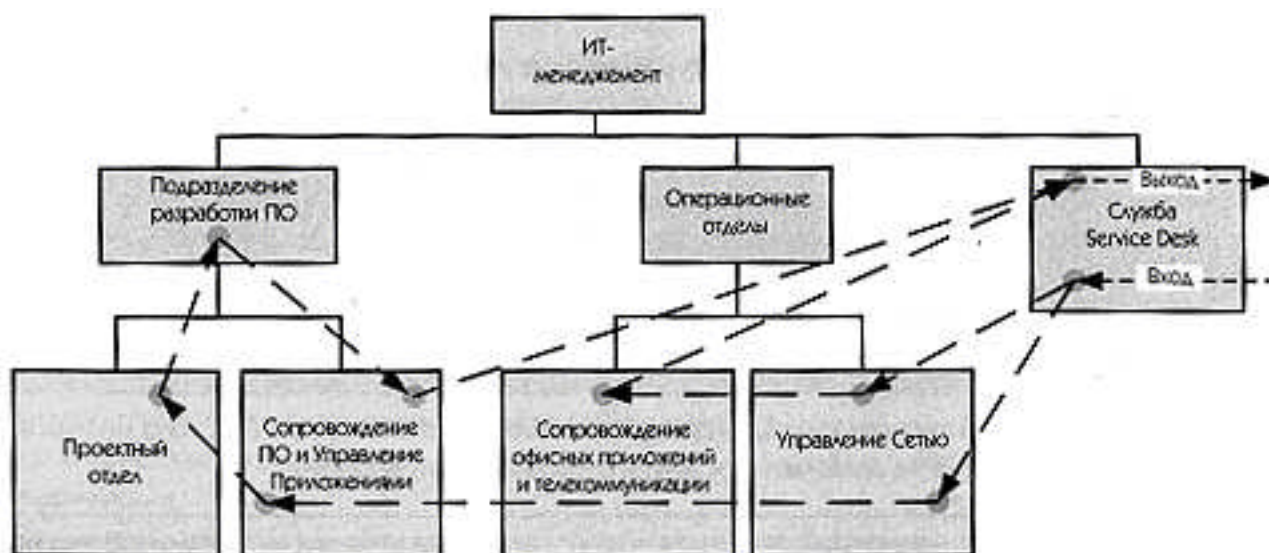
На рис. 2.9 представлена модель процесса, созданная с использованием подхода ITIL. Эта модель является основой процессов ИТ Сервис-менеджмента, описанных в этой книге.



2.3.2. Процессы и организационные подразделения

Большинство компаний имеют иерархическую структуру. Они состоят из подразделений, объединяющих группы сотрудников. Существуют разные принципы формирования подразделений, например, по типу заказчика, продукту, региону или области знания. Как правило, в предоставлении ИТ-услуг (сервисов) участвуют одновременно несколько отделов и затрагиваются несколько областей знаний. Например, если существует ИТ-сервис по предоставлению доступа к программе бухгалтерского учета на центральном компьютере, то в это будет вовлечено несколько подразделений. Вычислительный центр должен будет обеспечить доступ к программе и базе данных, служба передачи данных и телекоммуникаций будет обеспечивать связь с вычислительным центром, а подразделение поддержки персональных компьютеров — предоставлять пользователям интерфейс для доступа к программе.

В процессах, в которых участвует несколько подразделений, контроль качества услуг осуществляется путем мониторинга определенных аспектов качества, например таких, как доступность, мощность¹ ИТ-средств (пропускная способность), стоимость и стабильность. Затем ИТ-организация сопоставляет результаты мониторинга качества с потребностями заказчика. Структура таких процессов гарантирует получение качественной информации о предоставлении услуг, так, чтобы можно было совершенствовать контроль и планирование услуг.



2.3.3. ИТ Сервис-менеджмент

ИТ Сервис-менеджмент в первую очередь известен как ориентированный на процессы и услуги подход, который использовался в области, ранее известной как ИТ-менеджмент. В этой главе показано, что у процессов всегда должна быть определена цель. В свою очередь, цель процессов ИТ Сервис-менеджмента — содействовать повышению качества ИТ-услуг. Управление Качеством и контроль процессов являются частью организации и ее политики.

При процессно-ориентированном подходе необходимо учитывать ситуацию внутри организации (внутреннюю политику, корпоративную культуру, численность и так далее).

ITIL, наиболее известный подход к ИТ Сервис-менеджменту, не дает каких-либо ограничений по типу организации, а, наоборот, описывает связи между видами деятельности, составляющими процессы, которые применимы в организациях любого типа. Это создает структурированную основу² для обмена опытом между компаниями и изучения опыта динамично развивающихся организаций.

¹ Capacity.

² Framework.

Глава 3

Введение в ITIL

В данной главе описывается структура и задачи библиотеки передового опыта организации ИТ (ITIL)¹ и приводятся сведения об организациях, способствующих превращению ITIL в лучший практический стандарт для ИТ Сервис-менеджмента.

3.1. Общая картина

Библиотека ITIL была создана в результате осознания того факта, что достижение организациями своих корпоративных целей все более зависит от ИТ. Эта усиливающаяся зависимость привела к росту потребности в ИТ-услугах, качество которых отвечало бы целям бизнеса, требованиям и ожиданиям заказчика. С течением времени акцент переместился с разработки ИТ-приложений на Управление ИТ-услугами. ИТ-приложения (иногда называемые информационными системами) лишь тогда способствуют достижению корпоративных целей, когда система доступна пользователям, и при возникновении ошибок и необходимости модификации поддержка может быть оказана службой сопровождения.

В жизненном цикле ИТ-продуктов на их эксплуатацию приходится от 70 до 80% времени и финансовых средств, оставшаяся часть расходуется на разработку продукта (или его приобретение). Следовательно, для успешного использования ИТ существенное значение имеют эффективные и рациональные². Процессы Управления ИТ-услугами. Это относится к любому типу организаций, больших или малых, общественных или частных, с централизованными или децентрализованными ИТ-услугами, пользующихся аутсорсингом или работающих с внутренними ресурсами. В любом случае услуги должны быть надежными, согласующимися друг с другом, высококачественными и приемлемыми по стоимости.

ИТ Сервис-менеджмент рассматривает вопросы предоставления и поддержки ИТ-услуг, разработанных в соответствии с потребностями организации. Библиотека ITIL создавалась для систематического и последовательного распространения передового опыта по Управлению ИТ-услугами. Этот подход основывается на качестве услуг и разработке эффективных и рациональных процессов.

ITIL предлагает структурированную основу³ для организации всех видов деятельности в ИТ-под-разделении, являющихся частью оказания ИТ-услуг. Эти виды деятельности образуют процессы, составляющие основу для развития степени зрелости ИТ Сервис-менеджмента. Каждый из этих процессов решает одну или несколько задач ИТ-департамента, такие как разработка услуг (сервисов), Управление Инфраструктурой, предоставление и поддержка услуг. Такой процессный подход позволяет описать передовой опыт ИТ Сервис-менеджмента независимо от организационной структуры компании.

Многое из этого передового опыта легко заметно, и в той или иной степени уже используются в большинстве ИТ-организаций. Но библиотека ITIL представляет эти элементы практики в их связи ДРУГ с другом. В книгах ITIL описывается возможность оптимизации и улучшения координации между процессами. В них также объясняется, как эти процессы создают основу для введения общей терминологии внутри организации. Они помогают определить цели и усилия, необходимые для их решения.

Используя процессный подход, библиотека ITIL в первую очередь разъясняет, что должно включаться в ИТ Сервис-менеджмент в обязательном порядке для обеспечения ИТ-услуг необходимого качества. Структура и распределение заданий и ответственности между службами и отделами зависит от типа организации; эти структуры в ИТ-подразделениях могут быть разнообразными и часто меняться.

¹ Точным переводом названия «IT Infrastructure Library» является «Библиотека инфраструктуры информационных технологий», но, по мнению коллектива русской редакции, название «Библиотека передового опыта организации ИТ» более точно отражает ключевые принципы управления, используемые в мире при организации работы ИТ-подразделений, и отраженные в настоящее время в библиотеке ITIL

² Effective and efficient.

³ Framework.

Описание структуры процесса дает общий ориентир, который не столь быстро меняется, что может помочь в сохранении высокого качества ИТ-услуг во время и после проведения реорганизаций в компании, а также при смене поставщиков и партнеров.

Ниже приводятся некоторые достоинства и недостатки библиотеки ITIL. Этот список не претендует на полноту, но позволяет оценить преимущества и недостатки ITIL, а также демонстрирует, как ITIL может быть использован организациями.

Преимущества библиотеки ITIL для заказчиков/пользователей:

- предоставление ИТ-услуг становится более ориентированным на заказчика, соглашения о качестве услуг способствуют улучшению взаимоотношений;
- услуги описываются лучше, на языке заказчика и с требуемой детализацией;
- лучше контролируются качество и стоимость услуг;
- улучшается взаимосвязь компании с ИТ-организацией за счет определения точек контактов.

Преимущества библиотеки ITIL для ИТ-организаций:

- становится четко понятна структура ИТ-департамента, его организация становится более рациональной¹ и более ориентированной на корпоративные цели;
- руководство организацией становится более целенаправленным, облегчается Управление Изменениями;
- эффективная² структура процессов создает основу для эффективного аутсорсинга элементов ИТ-услуг;
- следование передовому опыту ITIL способствует изменению корпоративной культуры в направлении осознания, что задачей ИТ-департамента является предоставление услуг, и поддерживает внедрение системы обеспечения качества на основе стандартов серии ISO-9000;
- библиотека ITIL предоставляет единую «систему координат» и понятий для взаимодействия как в компании, так и с поставщиками, необходимую при разработке и стандартизации корпоративных процедур.

Возможные проблемы при работе с ITIL:

- переход на принципы ITIL может занять продолжительное время, потребовать значительных усилий и изменений в корпоративной культуре. Чересчур амбициозные планы при переходе на ITIL могут привести к разочарованию, и поставленные цели не будут достигнуты;
- если совершенствование структуры процессов становится самоцелью, может пострадать качество услуг. В этом случае процедуры становятся бюрократической преградой, которую сотрудники стараются по возможности избегать;
- улучшения не достигаются при недостатке понимания, что должны обеспечивать процессы (в чем их цель), что является критериями оценки эффективности процессов и как осуществлять их контроль.
- улучшения в предоставлении услуг и снижении стоимости недостаточно видны;
- успешная реализация требует вовлечения и наличие обязательств со стороны руководства и приверженности сотрудников на всех организационных уровнях.³ Предоставление права разработки структуры процессов специализированному подразделению может привести к его изоляции, в результате чего определенные им направления деятельности не будут приняты другими подразделениями;

¹ Efficient.

² Effective

³ Commitment of personnel at all levels in organization.

■ при недостаточных инвестициях в инструментальные средства (программное обеспечение и др.) процессы не будут работать должным образом и сервис не улучшится. Могут потребоваться дополнительные ресурсы и персонал, если организация уже перегружена текущей рутинной работой.

Эти возможные проблемы, конечно, могут быть решены. Библиотека ITIL развивалась с целью достижения преимуществ для ИТ-организации и компании в целом. Многие из лучших практических предложений направлены на предотвращение таких проблем или их решение в случае возникновения.

3.2. Организации

3.2.1. OGC(ССТА)

Библиотека ITIL первоначально была результатом работы Центрального агентства по вычислительной технике и телекоммуникациям (Central Computer and Telecommunications Agency — ССТА) при правительстве Великобритании. В апреле 2001 г. ССТА было объединено с Государственной торговой палатой (Office of Government Commerce — OGC), являющейся в настоящее время новым владельцем библиотеки ITIL. Целью OGC является помощь заказчикам из государственного сектора экономики Великобритании в модернизации их деятельности по закупкам и улучшении обслуживания путем максимального использования ИТ и других инструментариев. «Задачей OGC является модернизация закупок правительственными службами и работа по улучшению использования финансовых средств».¹ OGC способствует использованию «передового опыта»² в различных сферах деятельности (например, Управление Проектами, Управление Закупками и ИТ Сервис-менеджмент). OGC выпускает несколько книжных серий (библиотек), написанных экспертами из Великобритании и других стран мира, представляющими ряд компаний и организаций.

Принадлежащая OGC библиотека ITIL состоит из ряда доступных и детальных «Собраний практических руководств»³ для предоставления эффективных и рациональных⁴ ИТ-услуг (сервисов).

3.2.2. Форум itSMF

Форум по ИТ Сервис-менеджменту (Information Technology Service Management Forum — itSMF), ранее известный как Форум по менеджменту ИТ-инфраструктуры (Information Technology Infrastructure Management Forum — ITIMF) является единственной имеющей международное признание независимой группой пользователей⁵, занимающейся вопросами ИТ Сервис-менеджмента. Ее единственными владельцами и управляющими являются члены группы. Форум itSMF оказывает определяющее влияние и делает вклад в популяризацию передового опыта и разработку стандартов во всем мире. Первая региональная организация /itSMF возникла в Великобритании в 1991 г. Следующей была голландская (itSMF — The Netherlands), учрежденная в Нидерландах в 1993 г. Сейчас отделения форума itSMF есть в таких странах, как ЮАР, Бельгия, Германия/Австрия/Швейцария, Канада, США и Австралия; все они сотрудничают в рамках форума itSMF International. Сайты этих отделений указаны в приложении В2.

Региональные отделения itSMF способствуют обмену информацией и опытом, что позволяет ИТ-организациям повысить качество предоставляемых услуг. Они организуют семинары, конференции, обсуждения отдельных тем и другие мероприятия, посвященные современным проблемам ИТ Сервис-менеджмента. Кроме того, они издают информационные бюллетени и используют Web-сайты для обмена информацией. Рабочие группы⁶ способствуют дальнейшему развитию библиотеки ITIL.

¹ «OGC aims to modernize procurement in government, and deliver substantial value for money improvements».

² «Best practices».

³ "Codes of practice-Effective and efficient.

⁴ Effective and efficient.

⁵ User group.

⁶ Task forces.

3.2.3. Организации EXIN и ISEB

Голландская организация «Exameninstituut voor Informatica» (EXIN) и британская «Information Systems Examination Board» (ISEB) совместно разработали профессиональную систему сертификации в рамках библиотеки ITIL. Разработка проводилась в тесном сотрудничестве с OGC и itSMF. EXIN и ISEB являются некоммерческими организациями, сотрудничающими для разработки всего диапазона квалификационных сертификатов ITIL трех уровней:

- базовый сертификат по ИТ Сервис-менеджменту — Foundation Certificate in IT Service Management;
- сертификат специалиста по ИТ Сервис-менеджменту — Practitioner Certificate in IT Service Management]
- сертификат менеджера по ИТ Сервис-менеджменту — Manager Certificate in IT Service Management.

Система сертификации основана на требованиях по эффективному выполнению соответствующей роли в ИТ-организации. К настоящему времени базовые сертификаты получили более 50 000 профессионалов ИТ из более чем 30 стран.

Базовый сертификат предназначен для всего персонала, который должен быть в курсе главных задач ИТ-организации и их взаимосвязи. Экзамен на получение базового сертификата включает оценку знаний Службы Service Desk и Процессов Управления Инцидентами, Проблемами, Изменениями, Конфигурациями, Релизами, Уровнем Услуг, Доступностью, Мощностями, Непрерывностью ИТ-услуг и Финансами ИТ. После получения базового сертификата разрешается сдавать экзамены на получение сертификата специалиста и менеджера. Специалисты получают навыки практического осуществления отдельных ITIL-процессов и задач в рамках таких процессов, как Управление Инцидентами, Изменениями и Уровнем Услуг. Менеджеры получают теоретические знания о том, как управлять всеми процессами, перечисленными в базовом сертификате, как консультировать по структуре и оптимизации процессов и как осуществлять внедрение этих процессов.

Сегодня библиотека ITIL представляет собой гораздо большее, чем серию полезных книг по ИТ Сервис-менеджменту. В практический опыт ITSM в настоящее время входит вся индустрия, включающая организации, инструментарии (специализированное программное обеспечение), тренинговые и консалтинговые услуги, соответствующие методологические основы¹ и публикации. С 90-х годов библиотека ITIL считается уже не только структурированной основой, но также подходом и философией, разделяемой теми, кто использует в своей работе передовой опыт ITIL. В настоящее время ряд организаций ведут международное сотрудничество для продвижения библиотеки ITIL как признанного «де факто» стандарта ИТ Сервис-менеджмента.

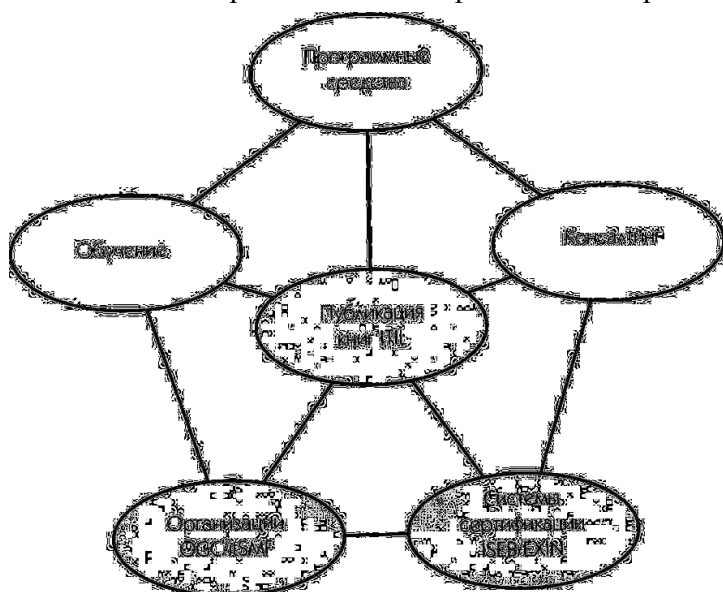


Рис. 3.1. Среда ITIL (источник: OGG)

¹ Frameworks.

На рис. 3.1 среда ITIL показывает, что привлеченные организации предоставляют обратную связь между текущей практикой (светлые эллипсы) и теорией (темные эллипсы) для поддержания актуальности библиотеки ITIL. Более того, разработаны расширения и альтернативные решения, отдельные из которых могут рассматриваться как самостоятельные методы ИТ Сервис-менеджмента. Эти альтернативные решения часто рассматривают вопросы определенных групп пользователей или организаций, специфические проблемы которых не находят адекватного отражения в ITIL. Уникальной особенностью библиотеки ITIL является то, что она предлагает общую основу¹, базирующуюся на практическом опыте профессиональных пользователей по всему миру.

3.3. Книги библиотеки ITIL

Каждая из книг библиотеки ITIL рассматривает вопросы отдельной части структурированной процессной основы. В них дается описание того, что необходимо для организации ИТ Сервис-менеджмента.

Библиотека ITIL определяет цели и виды деятельности, входные и выходные параметры каждого из процессов в ИТ-организации. Однако, библиотека ITIL не дает конкретного описания способов осуществления этой деятельности, так как они могут различаться в каждой организации. Акцент делается на проверенном практикой подходе, который может быть реализован различными способами в зависимости от обстоятельств. Библиотека ITIL не является методом; наоборот, она предлагает структурированную основу для планирования наиболее часто используемых процессов, ролей и видов деятельности, определяя связи между ними и необходимые виды коммуникации. Создание библиотеки ITIL вызвано необходимостью предоставления высококачественных услуг, уделяя при этом особое внимание отношениям с заказчиком. ИТ-организация должна выполнять соглашения с заказчиком, что означает поддержание хороших отношений с заказчиками и партнерами, такими, как поставщики.

Частично философия библиотеки ITIL имеет в своей основе системы качества, такие, как стандарты серии ISO-9000, и общие схемы обеспечения качества (Total Quality frameworks), как предлагаемые Европейской организацией Управления Качеством (European Foundation of Quality Management — EFQM). Библиотека ITIL поддерживает эти системы путем предоставления четкого описания процессов и передового опыта ИТ Сервис-менеджмента. Это может значительно сократить время, необходимое для прохождения сертификации ISO.

Первоначально библиотека ITIL состояла из нескольких комплектов книг, в каждом из которых описывалась конкретная область сопровождения и эксплуатации ИТ-инфраструктуры. Ядром ITIL считались десять книг, в которых описывались такие области, как поддержка услуг² и предоставление услуг³. Библиотека включала также около 40 других книг по вспомогательным предметам, имевшим отношение к ИТ Сервис-менеджменту, от монтажа кабелей до Управления Отношениями с Заказчиком. Однако, в первоначальных сериях книг вопросы ИТ Сервис-менеджмента рассматривали главным образом с точки зрения ИТ. Для заполнения разрыва между бизнес-практикой и ИТ-организацией в библиотеку была включена серия книг, рассматривающая бизнес-аспекты ИТ Сервис-менеджмента⁴. Более того, в определенных частях библиотеки ITIL в то время использовался несколько устаревший подход.

В настоящее время была сделана переработка центральных книг по ITIL и они были переизданы в виде двух книг: одна — по поддержке услуг и другая — по их предоставлению. Это позволило исключить повторы и встречающуюся местами несогласованность ранних серий, что улучшило структурное единство издания, которое теперь дает более четкое представление об ИТ Сервис-менеджменте.

¹ Generic framework.

² Service Support.

³ Service Delivery.

⁴ Business Perspective Set

Начатый после выпуска указанного издания пересмотр всей серии публикаций ITIL еще не завершен.



Рис. 3.2. Представление элементов библиотеки ITIL(источник: OGG)

Структурированный подход, изложенный в библиотеке ITIL, состоит из семи элементов (см. рис. 3.2). Все элементы взаимодействуют между собой и в определенной степени перекрываются друг с другом.

Этими элементами являются:

- Поддержка услуг (Service Support) — публикация 2000 г.;
- Предоставление услуг (Service Delivery) — публикация 2001 г.;
- Управление Инфраструктурой информационных и коммуникационных технологий (ICT Infrastructure Management) — публикация 2002 г.;
- Управление Приложениями (Applications management) — публикация 2002 г.;
- Управление Безопасностью (Security management) — публикация 2002 г.;
- Планирование внедрения Сервис-менеджмента (Planning to Implement Service Management) - публикация 2002 г.;
- Бизнес-перспектива (The Business Perspective) — публикация планируется в 2004 г.

В этой главе мы представляем серии публикаций ITIL. В течение 2002 г. оригинальная серия, первые книги которой появились в 1989 г., была заменена шестью новыми книгами ITIL, издание седьмой книги планируется на 2004 г. Более подробная информация по этой теме приводится в приложении и на Web-сайтах OGC и EXIN.

3.3.1. Предоставление услуг

Как уже отмечалось, Поддержка услуг и Предоставление услуг считаются центральными компонентами передового опыта ITIL для ИТ Сервис-менеджмента.

В книге ITIL по Предоставлению услуг описываются требования, необходимые для оказания услуг. В этой серии рассматриваются следующие вопросы:

- Управление Уровнем Услуг;
- Управление Финансами ИТ;
- Управление Мощностями;
- Управление Непрерывностью ИТ-услуг;
- Управление Доступностью.

В данную ознакомительную книгу было включено также Управление Информационной Безопасностью (со ссылкой на книгу ITIL по информационной безопасности), но оно не является частью серии по предоставлению услуг.

Сложную взаимосвязь между процессами, описываемыми в книгах по Поддержке и Предоставлению услуг, почти невозможно отобразить графически. В общих чертах они показаны в виде упрощенной схемы на рис. 3.3.

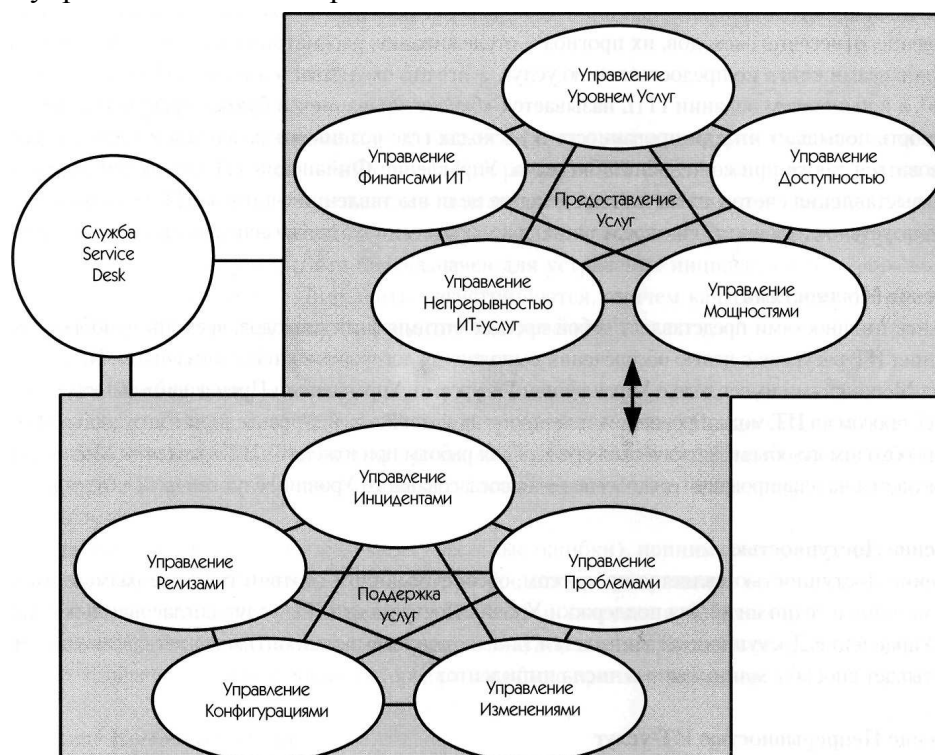


Рис. 3.3. Поддержка и предоставление Услуг

Управление Уровнем Услуг

Целью Управления Уровнем Услуг является достижение ясных соглашений с заказчиком об ИТ-услугах и реализация этих соглашений. Соответственно, для Управления Уровнем Услуг необходима информация о потребностях заказчика, о предоставляемых ИТ-организацией технических средствах и о имеющихся финансовых ресурсах.

Управление Уровнем Услуг рассматривает услуги, предоставляемые заказчику (с акцентом на заказчике¹). ИТ-организация может повысить степень удовлетворенности заказчика через создание услуг на основе его потребностей (услуги, вызванные спросом²), только на базе своих технических возможностей (услуги, вызванные предложением³). В главе об Управлении Уровнем Услуг книги по Предоставлению услуг рассматриваются следующие вопросы:

- как оптимизировать ИТ-услуги для их предоставления заказчикам по доступным ценам на основе точного определения договоренностей в Соглашении об Уровне Услуг;
- как проводить мониторинг и обсуждение услуг;
- как организовать Поддержку Услуг Внешними Договорами с поставщиками.

Управление Финансами ИТ

Управление Финансами касается экономических вопросов предоставляемых ИТ-услуг. Например, Процесс Управления Финансами подготавливает информацию о расходах, возникших при предоставлении услуг. В результате при определении необходимых изменений ИТ-инфраструктуры или ИТ-услуг возможен учет финансовых факторов (соотнесение расходов и доходов — цены и результата). Определение, отнесение расходов, их прогноз и отслеживание, рассматривавшиеся в главе об управлении финансами книги по

¹ Customer Focus.

² Demand pull

³ Supply push.

предоставлению услуг, — все это охватывается термином «расчет себестоимости»¹, а в нынешнем издании ITIL называется «бюджетированием и бухгалтерским учетом». Эта деятельность повышает информированность о расходах (где возникают издержки и какие) и может использоваться также при составлении бюджета. Управление Финансами ИТ описывает различные методы выставления счетов, включая определение цели выставления счетов за ИТ-услуги (для чего это используется в компании?) и определение ценообразования, а также аспекты бюджетирования.

Управление Мощностями

Управление Мощностями представляет собой процесс оптимизации расходов, времени приобретения и размещения ИТ-ресурсов с целью обеспечения выполнения договоренностей с заказчиком. Процесс Управления Мощностями имеет дело с Управлением Ресурсами, Управлением Производительностью, Управлением Спросом на ИТ, моделированием, планированием мощностей, Управлением Нагрузкой и определением необходимого объема технических средств для работы приложений². В Управлении Мощностями акцент делается на планировании для обеспечения согласованного Уровня Услуг сейчас и в будущем.

Управление Доступностью

Управление Доступностью является процессом, обеспечивающим соответствующее размещение ресурсов, методов и технологий для поддержки Уровня Доступности ИТ-услуг, согласованных с заказчиком. Управление Доступностью занимается такими вопросами, как оптимизация обслуживания и разрабатывает способы минимизации числа инцидентов.

Управление Непрерывностью ИТ-услуг

Этот процесс касается подготовки и планирования способов устранения чрезвычайных ситуаций с ИТ-услугами в случае остановки бизнеса. Называвшийся в предыдущем издании ITIL «Планированием на случай чрезвычайных обстоятельств»³, этот процесс уделяет основное внимание связям между всеми компонентами, необходимым для защиты непрерывности деятельности компании при катастрофах (т. е. для Управления Непрерывностью Бизнеса), а также средствам предотвращения таких катастроф. Управление Непрерывностью ИТ-услуг является процессом планирования и координации технических, финансовых и управленческих ресурсов, необходимых для обеспечения непрерывности услуг после катастроф, в соответствии с договоренностью с заказчиком.

3.3.2. Поддержка услуг

В книге ITIL по поддержке услуг описывается, как заказчик может получить доступ к соответствующим услугам для поддержки своего бизнеса. Эта книга охватывает следующие области:

- Служба Service Desk;
- Управление Инцидентами;
- Управление Проблемами;
- Управление Конфигурациями;
- Управление Изменениями;
- Управление Релизами.

Служба Service Desk

¹ Costins.

² Application sizing

³ Contingency Planning.

Служба Service Desk является точкой контакта пользователя с ИТ-организацией. Ранее в книгах ITIL она называлась службой Help Desk. Основными задачами службы Help Desk были регистрация, решение и отслеживание инцидентов. Служба Service Desk имеет более широкие функции (например, получение Запросов на Изменения) и может выполнять действия, относящиеся к нескольким процессам.

Управление Инцидентами

Разграничение между инцидентами и проблемами вероятно является одним из самых известных, но не самых популярных вкладов библиотеки ITIL в развитие ИТ Сервис-менеджмента. Хотя это разграничение иногда может запутывать, но его главное достоинство заключается в установлении различия между быстрым восстановлением услуги и установлением причины инцидента и ее устранением. Процесс Управления Инцидентами предназначен для устранения инцидента и быстрого возобновления предоставления услуг. Инциденты регистрируются, причем качество регистрационной информации определяет эффективность ряда других процессов.

Управление Проблемами

Если есть подозрение на проблему в ИТ-инфраструктуре, то целью Процесса Управления Проблемами является установление корневой причины. Подозрение на существование проблемы может возникнуть из-за наличия инцидентов, но безусловно целью является предотвращение сбоев везде, где это возможно.

Когда причины установлены (определены известные ошибки), принимается бизнес-решение о том, необходимо ли делать улучшения в инфраструктуре для предотвращения возникновения новых инцидентов. Такие улучшения производятся путем подачи Запросов на Изменение¹. Необходимо обратить внимание на то, что определение Управления Проблемами, дающееся в ITIL, значительно отличается от определения, которое раньше было принято, например, в ИТ-индустрии США.

Управление Конфигурациями

Задачами Управления Конфигурациями являются контроль изменяющейся ИТ-инфраструктуры (стандартизация и мониторинг статуса), идентификация Конфигурационных Единиц (инвентаризация, верификация и регистрация), сбор и Управление Документацией по ИТ-инфраструктуре, а также предоставление информации об ИТ-инфраструктуре для всех других процессов.

Управление Изменениями

Управление Изменениями направлено на контроль проведения изменений в ИТ-инфраструктуре. Целью процесса является определение необходимых изменений и способов их проведения с минимальным негативным воздействием на ИТ-услуги, при одновременном обеспечении контроля (отслеживании) изменений посредством консультаций и координации действий со всей организацией. Изменения производятся по Запросу от Заказчика, из Процесса Управления Проблемами или из некоторых других процессов. Управление Изменениями тесно связано с деятельностью по мониторингу статуса элементов из Процесса Управления Конфигурациями. Внесение изменений производится согласно разработанной схеме, включающей определение, планирование, создание и испытание, принятие окончательного решения о проведении, внедрение и оценку.

¹ Request For Change.

Управление Релизами

Релизом называется набор Конфигурационных Единиц¹, которые совместно тестируются и вводятся в активную рабочую среду. Главной задачей Управления Релизами является обеспечение успешного развертывания релизов, включая интеграцию, проведение тестирования и хранение.

Управление Релизами обеспечивает гарантию того, что в использовании находятся только тестированные и корректные версии авторизованного программного и аппаратного обеспечения. Управление Релизами тесно связано с деятельностью по Управлению Конфигурациями и Управлению Изменениями. Реальное внесение изменений часто осуществляется через действия в рамках Процесса Управления Релизами.

3.3.3. Другие рассматриваемые процессы

Существуют два процесса, которые хотя и не являются модулями ITIL в сериях Предоставление услуг и Поддержка услуг, но связаны ссылками с другими модулями или с ключевыми пунктами других процессов. Управление Отношениями с Заказчиком ИТ является процессом, привлекающим все больше внимания, но пока не вошедшим в какой-либо модуль ITIL. Управление Информационной Безопасностью было описано в публикации ITIL 1999 г., но формально не является частью серии Предоставление услуг. Вопросам безопасности в этой книге посвящена отдельная глава.

Управление Взаимоотношениями с Заказчиком ИТ

Передовой опыт многих организаций показывает, что рекомендуется использовать стройный целенаправленный подход к организации взаимоотношений с заказчиками, структурированный на нескольких уровнях. Деятельность по Управлению Взаимоотношениями с Заказчиком ИТ включается в несколько процессов (см. также раздел 2.2.5). Служба Service Desk является первой точкой контакта для пользователей. Однако заказавший услугу клиент первоначально вступает во взаимодействие с Процессом Управления Взаимоотношениями с Заказчиком ИТ. Он помогает выстроить мост между ИТ-организацией, традиционно использующей технические подходы к работе, и заказчиками, работающими над решением бизнес-задач своего предприятия. Управление Взаимоотношениями с Заказчиком ИТ не является частью серии книг по Предоставлению услуг и не рассматривается в этой ознакомительной книге.

Управление Информационной Безопасностью

Целью Процесса Управления Информационной Безопасностью является защита ИТ-инфраструктуры от несанкционированного использования (например, от несанкционированного доступа к данным). Такая защита основана на требованиях безопасности, заложенных в соглашениях об Уровне Услуг, контрактных требованиях, законодательстве, правилах работы компании и базовом Уровне Безопасности. При подготовке новой редакции раздела ITIL по предоставлению услуг было решено, что недавно выпущенную книгу по Управлению Информационной Безопасностью не стоит заменять. Книга ITIL по предоставлению услуг не рассматривает данного предмета, но ссылается на книгу ITIL по Управлению Информационной Безопасностью.

¹ Configuration item (CI).

Глава 4

Управление Инцидентами

4.1. Введение

Задача Процесса Управления Инцидентами является реактивной — уменьшение или исключение отрицательного воздействия (потенциальных) нарушений в предоставлении ИТ-услуг, таким образом обеспечивая наиболее быстрое восстановление работы пользователей. Для выполнения этой задачи производится регистрация, классификация и назначение инцидентов соответствующим группам специалистов, мониторинг хода работ по разрешению инцидентов, решение инцидентов и их закрытие. Так как это требует тесного взаимодействия с пользователями, фокусной точкой Процесса Управления Инцидентами обычно является функция Service Desk¹, которая играет роль центра контактов пользователей с «внутренними» коллективами технических служб. Управление Инцидентами является важнейшей основой для работы других процессов ИТIL, предоставляя ценную информацию об ошибках в работе ИТ-инфраструктуры.

На рис. 4.1 показан схематичный пример Управления Инцидентами как горизонтальный процесс, охватывающий разные ИТ-отделы и осуществляющий эффективное управление и контроль обработки потока инцидентов.

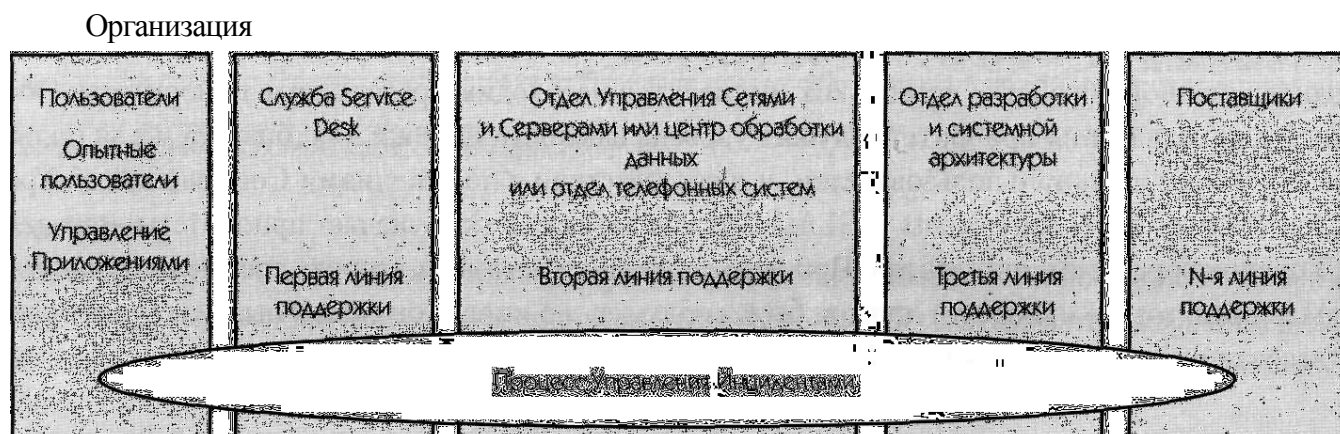


Рис. 4.1. Позиционирование Процесса Управления Инцидентами относительно других функций (подразделений) ИТ-организации.

4.1.1. Терминология

Инцидент

Библиотека ИТIL использует широкое определение термина «инцидент», поэтому почти все обращения пользователей могут регистрироваться и отслеживаться как инциденты.

В книге «Поддержка услуг» библиотеки ИТIL дается следующее определение:

Инцидент² — это любое событие, не являющееся частью стандартных операций по предоставлению услуги, которое привело или может привести к нарушению или снижению качества этой услуги.

В контексте библиотеки ИТIL инцидентами считаются не только ошибки аппаратного или программного обеспечения, но также и Запросы на Обслуживание.

Запрос на Обслуживание³ — это Запрос от Пользователя на поддержку, предоставление информации, консультации или документации, не являющийся сбоем ИТ-инфраструктуры.

Примеры Запросов на Обслуживание:

¹ В литературе по ИТIL понятие «функция» ассоциировано с вертикальным (линейным) подразделением организации, выполняющим соответствующие функциональные обязанности и фактически является его синонимом. — Прим. ред.

² Incident.

³ Service request

- вопрос о функционировании ИТ-систем или запрос о предоставлении какой-либо информации;
- запрос о состоянии (статусе) чего-либо в ИТ-инфраструктуре;
- запрос о замене пароля;
- запросы на выполнение пакетных заданий, восстановление или авторизацию пароля;
- получение информации из базы данных.

Для того чтобы можно было отличить «настоящие инциденты» от «инцидентов-Запросов на Обслуживание», рекомендуется присваивать Запросам на Обслуживание специальную категорию. Важно также отметить, что Запрос на Обслуживание это не то же самое, что Запрос на Изменение;

Запрос на Изменение (RFC)¹ — это экранная или бумажная форма, используемая для записи детальной информации о предлагаемом Запросе на Изменение какой-либо Конфигурационной Единицы² (CI) в ИТ-инфраструктуре или процедуры или какого-либо иного объекта ИТ-инфраструктуры.

Запрос на Изменение RFC считается завершенным после проведения изменения в инфраструктуре, например, замены зарегистрированных компонентов, инсталляции ПК и т. д. Это не инциденты, а изменения.

Степень воздействия³, срочность⁴ и приоритет⁵

При одновременной обработке нескольких инцидентов необходимо расставлять приоритеты. Обоснованием для назначения приоритета служит уровень важности ошибки для бизнеса и для пользователя. На основе диалога с пользователем и в соответствии с положениями Соглашений об Уровнях Услуг (Service Level Agreements — SLAs) Служба Service Desk назначает приоритеты, определяющие порядок обработки инцидентов. При эскалации инцидентов на вторую, третью или более линии поддержки, тот же приоритет должен быть соблюден, но иногда он может быть скорректирован по согласованию со Службой Service Desk.

Конечно, каждый пользователь будет считать, что его инцидент имеет наивысший приоритет, но мнения пользователей часто бывают субъективными. Для объективной оценки приоритета в диалоге с пользователем употребляются следующие критерии:

- **степень воздействия инцидента:** степень отклонения от нормального уровня предоставления услуги, выражающаяся в количестве пользователей или бизнес-процессов, подвергшихся воздействию инцидента;
- **срочность инцидента:** приемлемая задержка разрешения инцидента для пользователя или бизнес-процесса.

Приоритет определяется на основе срочности и степени воздействия. Для каждого приоритета определяется количество специалистов и объем ресурсов, которые могут быть направлены на разрешение инцидента. Порядок обработки инцидентов одинакового приоритета может быть определен в соответствии с усилиями, необходимыми для разрешения инцидента. Например, легко разрешаемый инцидент может быть обработан перед инцидентом, требующим больших усилий.

При Управлении Инцидентами существуют способы снижения степени воздействия и срочности, такие, как переключение системы на резервную конфигурацию, перенаправление очереди печати и др.

1 Request for change — RFC. 9

2 Configuration item — CI

3 Impact.

4 Urgency.

5 Priority.

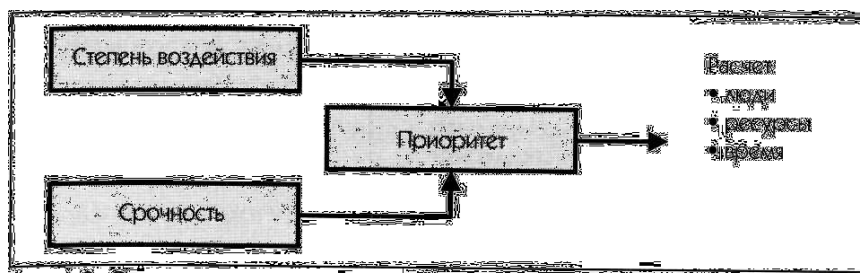


Рис. 4.2. Определение степени воздействия, срочности и приоритета

Степень воздействия и срочность также могут сами меняться во времени, например при росте количества пользователей, подвергшихся воздействию инцидента или в критические моменты времени.

Степень воздействия и срочность могут быть объединены в матрицу, например, как показано в табл. 4.1.

		СТЕПЕНЬ ВОЗДЕЙСТВИЯ		
СРОЧНОСТЬ	Приоритет	Высокая	Средняя	Низкая
	Время разрешения			
	Высокая	Критический < 1 часа	Высокий < 8 часов	Средний < 24 часов
	Средняя	Высокий < 8 часов	Средний < 24 часов	Низкий < 48 часов
	Низкая	Средний < 24 часов	Низкий < 48 часов	Планирование Запланировано

Таблица 4.1. Пример системы кодирования приоритетов

Эскалация

Если инцидент не может быть разрешен первой линией поддержки за согласованное время, необходимо привлечение дополнительных знаний или полномочий. Это называется эскалацией, которая происходит в соответствии с рассмотренными выше приоритетами и, соответственно, временем разрешения инцидента. Различают функциональную и иерархическую эскалацию:

- **Функциональная эскалация** (горизонтальная) — означает привлечение большего количества специалистов или предоставление дополнительных прав доступа для разрешения инцидента; при этом, возможно, происходит выход за пределы одного структурного ИТ-подразделения.

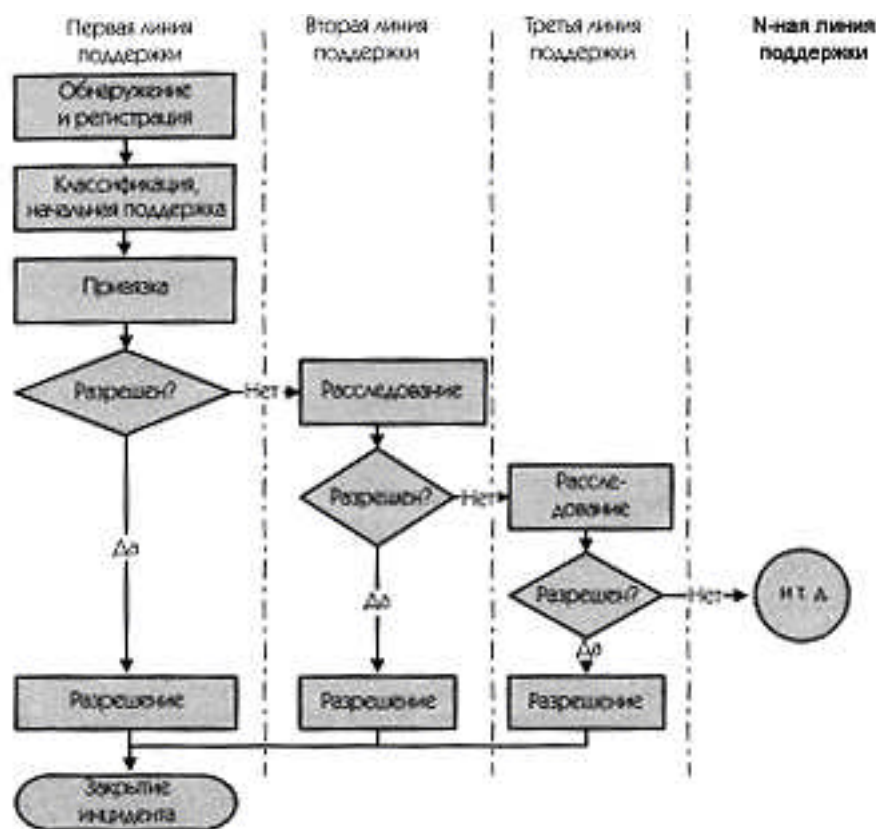
- **Иерархическая эскалация** (вертикальная) — означает вертикальный переход (на более высокий уровень) в рамках организации, так как для разрешения инцидента недостаточно организационных полномочий (уровня власти) или ресурсов.

Задачей Руководителя Процесса Управления Инцидентами является заблаговременное резервирование возможностей для функциональной эскалации в рамках линейных подразделений организации так, чтобы разрешение инцидентов не требовало регулярной иерархической эскалации. В любом случае, линейные подразделения должны предоставить для этого процесса достаточное количество ресурсов.

Первая, вторая и n-линия поддержки

Выше была изложена маршрутизация инцидента, или функциональная эскалация. Маршрутизация определяется требуемым уровнем знаний, полномочий и срочностью. Первой линией поддержки (называемой также поддержкой 1-го уровня) обычно является Служба Service Desk, второй линией — подразделения, осуществляющие Управление ИТ-инфраструктурой, третья — отделы разработки и архитектуры программного обеспечения, и

четвертая — поставщики. Чем меньше организация, тем меньше в ней уровней эскалации. В больших организациях Руководитель Процесса Управления Инцидентами может назначить Координаторов инцидентов в соответствующих подразделениях для поддержки своей деятельности. Например, координаторы могут играть роль интерфейса между процессной деятельностью и линейными организационными подразделениями. Каждый из них координирует деятельность собственных групп поддержки. Процедура эскалации графически представлена на рис. 4.3.



4.2. Цель

Целью Процесса Управления Инцидентами является скорейшее восстановление нормального Уровня Услуг, определенного в Соглашении об Уровне Услуг (Service Level Agreement — SLA), с минимальными возможными потерями для бизнес-деятельности организации и пользователей. Кроме того, Процесс Управления Инцидентами должен вести точную регистрацию инцидентов для оценки и совершенствования процесса и предоставления необходимой информации для других процессов.

4.2.1. Преимущества использования процесса

- Для бизнеса в целом:
 - своевременное разрешение инцидентов, ведущее к уменьшению потерь для бизнеса;
 - повышение производительности работы пользователей;
 - независимый, ориентированный на потребности заказчика мониторинг инцидентов;
 - доступность объективной информации о соответствии предоставляемых услуг согласованным договоренностям (SLA).
- Для ИТ-организации:
 - улучшенный мониторинг, позволяющий проводить точное сопоставление уровня производительности ИТ-систем с соглашениями (SLA);
 - эффективное руководство и мониторинг выполнения соглашений (SLA) на основе достоверной информации;
 - эффективное использование персонала;

- предотвращение потерь инцидентов и Запросов на Обслуживание или их неправильной регистрации;
- повышение точности информации в Конфигурационной Базе Данных (Configuration Management Database — CMDB) за счет ее проверки при регистрации инцидентов в привязке к Конфигурационным Единицам (Configuration Item — CI);
- повышение удовлетворенности пользователей и заказчиков.

Отказ от использования Процесса Управления Инцидентами может привести к следующим отрицательным последствиям:

- инциденты могут быть потеряны или, наоборот, необоснованно восприняты как чрезвычайно серьезные из-за отсутствия ответственных за мониторинг и эскалацию, что может привести к снижению общего уровня обслуживания;
- пользователи могут перенаправляться к одним и тем же специалистам «по кругу» без успешного разрешения инцидента;
- специалисты могут постоянно отрываться от работы телефонными звонками пользователей, из-за чего им становится трудно эффективно выполнять свою работу;
- могут возникать ситуации, когда несколько человек будут работать над одним и тем же инцидентом, непродуктивно теряя время, и примут противоречивые решения;
- может ощущаться недостаток информации о пользователях и предоставляемых услугах, необходимой для принятия руководящих решений;
- из-за указанных выше возможных проблем затраты компании и ИТ-организации на поддержку услуг будут выше, чем реально требуется.

4.3. Процесс

На рис. 4.4 показаны входы и выходы процесса, а также виды деятельности, которые охватывает этот процесс.

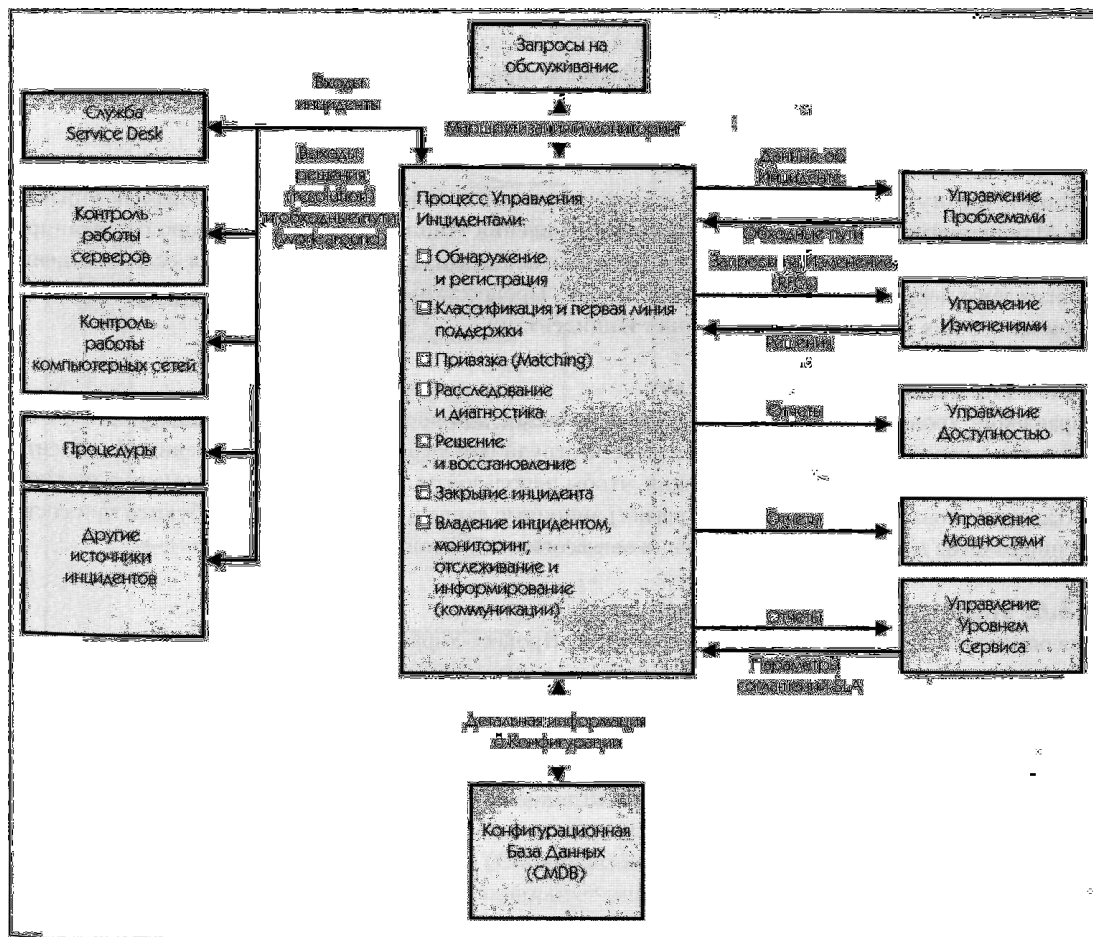


Рис. 4.4. Положение Процесса Управления Инцидентами

4.3.1. Входы процесса

Инциденты могут возникнуть в любой части инфраструктуры. Часто о них сообщают пользователи, но возможно их обнаружение и сотрудниками других отделов, а также автоматическими системами управления, настроенными на регистрацию событий в приложениях и технической инфраструктуре.

4.3.2. Управление Конфигурациями

Конфигурационная База Данных (Configuration Management Database — CMDB) играет важную роль в Управлении Инцидентами, так как она определяет связь между ресурсами, услугами, пользователями и Уровнями Услуг (сервисов). Например, Управление Конфигурациями показывает, кто является ответственным за компонент инфраструктуры, что делает возможным более эффективное распределение инцидентов по группам специалистов. Кроме того, эта база данных помогает решать оперативные вопросы, например, перенаправление очереди печати или переключение пользователя на другой сервер. При регистрации инцидента в регистрационные данные добавляется связь (link) с соответствующей Конфигурационной Единицей (Configuration Item — CI), позволяющая предоставить более подробную информацию об источнике ошибки. В случае необходимости может быть обновлен статус соответствующей компоненты в CMDB.

4.3.3. Управление Проблемами

Эффективное Управление Проблемами требует качественной регистрации инцидентов, что значительно облегчит поиск корневых причин. С другой стороны, Управление Проблемами помогает Процессу Управления Инцидентами, предоставляя информацию о проблемах, известных ошибках, обходных решениях и быстрых исправлениях¹.

4.3.4. Управление Изменениями

Инциденты могут быть решены путем внесения изменений, например, заменой монитора. Управление Изменениями предоставляет Процессу Управления Инцидентами информацию о запланированных изменениях и их статусах. Кроме того, изменения могут вызвать инциденты, если изменения произведены неправильно или содержат ошибки. Процесс Управления Изменениями получает информацию о них из Процессы Управления Инцидентами.

4.3.5. Управление Уровнем Услуг

Управление Уровнем Услуг контролирует выполнение договоренностей (соглашений — SLA) с заказчиком о предоставляемой ему поддержке. Сотрудники, участвующие в Управлении Инцидентами должны хорошо знать эти соглашения, чтобы использовать необходимую информацию при контактах с пользователями. Кроме того, регистрационные данные об инцидентах требуются при составлении отчетов для проверки выполнения согласованного Уровня Услуг.

4.3.6. Управление Доступностью

Для определения показателей доступности услуг Процесс Управления Доступностью использует регистрационные данные об инцидентах и данные мониторинга статуса, предоставляемые Процессом Управления Конфигурациями. Аналогично Конфигурационной Единице (CI) в Конфигурационной Базе Данных (CMDB), сервису (услуге) может быть также назначен статус «не работает»². Это может быть использовано для проверки действительных показателей доступности услуги и времени реагирования поставщика. При осуществлении такой проверки необходима фиксация времени действий, произошедших в процессе обработки инцидента, от момента обнаружения и до закрытия.

4.3.7. Управление Мощностями

¹ Quick Fixes

² «Down»

Процесс Управления Мощностями получает информацию об инцидентах, связанных с функционированием самих ИТ-систем, например, инцидентах, произошедших в связи с недостатком дискового пространства или медленной скоростью реакции и т. д. В свою очередь, информация об этих инцидентах может поступать в Процесс Управления Инцидентами от системного администратора или от самой системы на основе мониторинга своего состояния. На рис. 4.5 показаны этапы процесса:

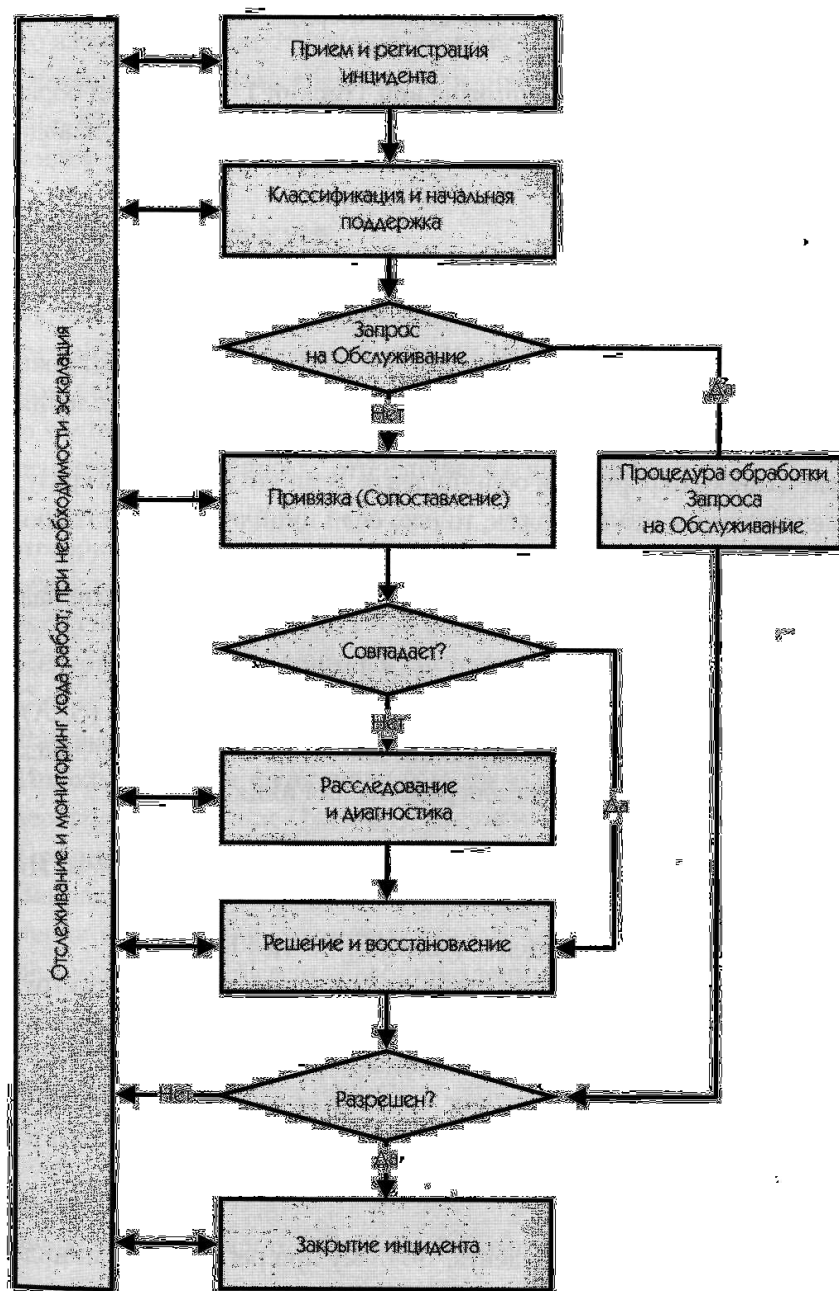


Рис. 4.5. Процесс Управления Инцидентами

- Прием и регистрация инцидента (Acceptance and Recording) — принимается сообщение и создается запись об инциденте.
- Классификация и начальная поддержка (Classification and Initial support) — присваиваются тип, статус, степень воздействия, срочность, приоритет инцидента, SLA и т. п. Пользователю может быть предложено возможное решение, даже если оно только временное.
- Если вызов касается **Запроса на Обслуживание** (Service Request), то инициируется соответствующая процедура.
- Привязка (или сопоставление — Matching) — проверяется, не является ли инцидент уже известным инцидентом или известной ошибкой, нет ли для него уже открытой проблемы, и нет ли для него известного решения или обходного пути.

- **Расследование и диагностика** (Investigation and Diagnosis) — при отсутствии известного решения производится исследование инцидента с целью как можно быстрее восстановить нормальную работу.
- **Решение и восстановление** (Resolution and Recovery) — если решение найдено, то работа может быть восстановлена.
- **Закрытие** (Closure) — с пользователем связываются, чтобы он подтвердил согласие с предложенным решением, после чего инцидент может быть закрыт.
- **Мониторинг хода работ и отслеживание** (Progress monitoring and Tracking) — весь цикл обработки инцидента контролируется, и если инцидент не может быть разрешен вовремя, производится эскалация.

4.4. Виды деятельности 4.4.1. Прием и регистрация

В большинстве случаев инциденты регистрируются Службой Service Desk, куда поступают сообщения о них. Регистрация всех инцидентов должна производиться немедленно после поступления сообщения по следующим причинам:

- трудно произвести точную регистрацию информации об инциденте, если это не сделано сразу;
- мониторинг хода работ по решению инцидента возможен, только если инцидент зарегистрирован;
- зарегистрированные инциденты помогают при диагностике новых инцидентов;
- Управление Проблемами может использовать зарегистрированные инциденты при работе над поиском корневых причин;
- легче определить степень воздействия, если все сообщения (звонки) зарегистрированы;
- без регистрации инцидентов невозможно контролировать исполнение договоренностей (SLA);
- немедленная регистрация инцидентов предотвращает ситуации, когда или несколько человек работают над одним звонком, или никто ничего не делает для разрешения инцидента.

Место обнаружения инцидента определяется по признаку, откуда пришло сообщение о нем. Инциденты могут быть обнаружены следующим образом:

- **Обнаружен пользователем:** он докладывает об инциденте в Службу Service Desk.
- **Обнаружен системой:** при обнаружении события в приложении или технической инфраструктуре, например, при превышении критического порога, событие регистрируется как инцидент в системе регистрации инцидентов и, при необходимости, направляется в группу поддержки.
- **Обнаружен сотрудником Службы Service Desk:** сотрудник производит регистрацию инцидента.
- **Обнаружен кем-либо в другом подразделении ИТ:** этот специалист регистрирует инцидент в системе регистрации инцидентов или докладывает о нем в Службу Service Desk.

Необходимо избегать двойной регистрации одного инцидента. Поэтому при регистрации инцидента следует проверить, нет ли аналогичных открытых инцидентов:

- Если есть (и они касаются того же инцидента), информация об инциденте обновляется или же инцидент регистрируется отдельно и устанавливается связь (привязка) к главному инциденту; при необходимости изменяется степень воздействия и приоритет, и добавляется информация о новом пользователе.
- Если нет (отличается от открытого инцидента), производится регистрация нового инцидента.
- В обоих случаях продолжение процесса одинаково, хотя в первом случае последующие действия гораздо проще.

При регистрации инцидента производятся следующие действия:

- **Назначение номера инцидента:** в большинстве случаев система автоматически назначает новый (уникальный) номер инцидента. Часто этот номер сообщается пользователю, чтобы он мог ссылаться на него при дальнейших контактах.
- **Запись базовой диагностической информации:** время, признаки (симптомы), пользователь, сотрудник, принявший вопрос в обработку, место произошедшего инцидента и информация о затронутой услуге и/или технических средствах.
- **Запись дополнительной информации об инциденте:** добавляется информация, например, из скрипта (script) или процедуры опроса или из Конфигурационной Базы Данных — CMDB (обычно на основе взаимоотношений Конфигурационных Единиц, определенных в CMDB).
- **Объявление сигнала тревоги:** если происходит инцидент, имеющий высокую степень воздействия, например, сбой важного сервера, производится предупреждение других пользователей и руководства.

4.4.2. Классификация

Классификация инцидентов направлена на определение его категории для облегчения мониторинга и составления отчетов. Желательно, чтобы опции классификации были как можно шире, но при этом требуется более высокий уровень ответственности персонала. Иногда пытаются объединить в одном перечне несколько аспектов классификации, таких, как тип, группа поддержки и источник. Это часто вносит путаницу. Лучше использовать несколько коротких перечней. В данном разделе рассматриваются вопросы, относящиеся к классификации.

Категория

Прежде всего, инцидентам присваивается категория и подкатегория, например, исходя из предполагаемого источника инцидента или соответствующей группы поддержки:

- **Центральная процессинговая система** — подсистема доступа, центральный сервер, приложение.
- **Сеть** — маршрутизаторы, сегменты, концентратор (hub), IP-адреса.
- **Рабочая станция** — монитор, сетевая карта, дисковод, клавиатура.
- **Использование и функциональность** — услуга (сервис), возможности системы, доступность, резервное копирование (back-up), документация.
- **Организация и процедуры** — заказ, запрос, поддержка, оповещение (коммуникации).
- **Запрос на Обслуживание** — запрос пользователя в Службу Service Desk на поддержку, предоставление информации, документации или оказание консультации. Это может быть выделено в отдельную процедуру или обработано таким же образом, как реальный инцидент.

Приоритет

После этого назначается приоритет, чтобы быть уверенными, что группа поддержки уделит инциденту необходимое внимание. Приоритет — это номер, определяющийся срочностью (насколько быстро это должно быть исправлено) и степенью воздействия (какой ущерб будет нанесен, если не исправить быстро). Приоритет = Срочность x Степень воздействия.

Услуги (сервисы)

Для определения услуг, подвергшихся воздействию инцидента, может быть использован перечень существующих договоренностей (соглашений) об Уровне Услуг — SLA. Этот перечень позволит также установить время эскалации для каждой из услуг, определенных в SLA.

Группа поддержки

Если Служба Service Desk не может разрешить инцидент незамедлительно, то определяется группа поддержки, которая будет заниматься разрешением инцидента. Основой для распределения

(маршрутизации) инцидентов часто является информация о категориях. При определении категорий может потребоваться рассмотрение структуры групп поддержки. Правильное распределение инцидентов имеет существенное значение для эффективности Процесса Управления Инцидентами. Поэтому одним из ключевых показателей эффективности¹ (KPI) Процесса Управления Инцидентами может быть число неправильно распределенных обращений.

Сроки решения

С учетом приоритета и соглашения SLA пользователь информируется о максимальном расчетном времени разрешения инцидента. Эти сроки также фиксируются в системе.

Идентификационный номер инцидента

Абонент информируется о номере инцидента для его точной идентификации при последующих обращениях.

Статус

Статус инцидента указывает на его положение в процессе обработки инцидента. Примерами статусов могут быть:

- новый;
- принят;
- запланирован;
- назначен;
- активный;
- отложен;
- разрешен;
- закрыт.

4.4.3. Привязка (сопоставление)

После классификации проводится проверка, не возникал ли аналогичный инцидент ранее и нет ли готового решения или обходного пути. Если инцидент имеет те же признаки, что и открытая проблема или известная ошибка, то может быть установлена связь с ними.

4.4.4. Расследование и диагностика

Служба Service Desk или группа поддержки направляет инциденты, не имеющие готового решения или выходящие за пределы компетенции работающего с ним сотрудника, группе поддержки следующего уровня с большим опытом и знаниями. Эта группа исследует и разрешает инцидент или направляет его группе поддержки очередного уровня.

В процессе разрешения инцидента различные специалисты могут обновлять регистрационную запись о нем, изменяя текущий статус, информацию о выполненных действиях, пересматривая классификацию и обновляя время и код работавшего сотрудника.

4.4.5. Решение и восстановление

После успешного завершения анализа и разрешения инцидента сотрудник записывает решение в сие тему. В некоторых случаях необходимо направить Запрос на Изменение (RFC) в Процесс Управления Изменениями. В наихудшем случае, если не найдено никакого решения, инцидент остается открытым»

4.4.6. Закрытие

¹ Key Performance Indicators - KPI

После реализации решения, удовлетворяющего пользователя, группа поддержки направляет инцидент обратно в Службу Service Desk. Эта служба связывается с сотрудником, сообщившим об инциденте, целью получения подтверждения об успешном решении вопроса. Если он это подтверждает, то инцидент может быть закрыт; в противном случае процесс возобновляется на соответствующем уровне. При закрытии инцидента необходимо обновить данные об окончательной категории, приоритете, сервисах (услугах), подвергшихся воздействию инцидента и Конфигурационной Единице (CI), вызвавшей сбой.

4.4.7. Мониторинг хода решения и отслеживание

В большинстве случаев ответственной за мониторинг хода решения является Служба Service Desk, как «владелец» всех инцидентов. Эта служба должна также информировать пользователя о состоянии инцидента. Обратная связь с пользователем может быть уместной после изменения статуса, например, направлении инцидента на следующую линию поддержки, изменении расчетного времени решения, эскалации и т. д. Во время мониторинга возможна функциональная эскалация к другим группам поддержки или иерархическая эскалация для принятия руководящих решений.

4.5. Контроль процесса

Основой контроля процесса являются отчеты для различных целевых групп. Руководитель Процесса Управления Инцидентами является ответственным за эти отчеты, а также за составление списка рассылки и графика составления отчетов. Отчеты могут включать специализированную информацию для следующих функциональных подразделений:

- **Руководителю Процесса Управления Инцидентами отчет необходим для:**

- идентификации недостающих звеньев процесса;
- идентификации нарушений исполнения соглашений об Уровне Услуг (SLA);
- отслеживания хода выполнения процесса;
- определения тенденций развития.

- **Руководство Линейными ИТ-подразделениями** — отчет для руководства группы поддержки; он также может быть полезен в Управлении ИТ-подразделениями. Отчет должен содержать следующую информацию:

- прогресс в решении инцидентов;
- время разрешения инцидентов в различных группах поддержки.

- **Управления Уровнем Сервисов (Услуг)** — отчет должен, прежде всего, содержать информацию о качестве предоставляемых услуг. Руководитель Процесса Управления Уровнем Услуг должен получать всю информацию, необходимую для составления Отчетов об Уровне Услуг перед заказчиками. Отчеты для заказчиков должны предоставлять информацию о том, выполняются ли соглашения в отношении Уровня Сервисов (услуг) в рамках Процесса Управления Инцидентами.

- **Руководителей других процессов ИТ Сервис-менеджмента** — отчеты для руководителей других процессов должны быть, в первую очередь, информативными, то есть содержать всю необходимую им информацию. Например, Процесс Управления Инцидентами на основе регистрационных записей об инцидентах может предоставлять следующую информацию:

- число обнаруженных и зарегистрированных инцидентов;
- число разрешенных инцидентов, с разделением по времени разрешения;
- статус и число неразрешенных инцидентов;
- инциденты с разбивкой по периодам возникновения, группам заказчика, группам поддержки и временем разрешения в соответствии с соглашением (SLA);
- инциденты с разбивкой по категориям, приоритетам и группам поддержки и др.

4.5.1. Критические факторы успеха

Для успешного Управления Инцидентами необходимо следующее:

- Актуальная Конфигурационная База Данных (CMDB), помогающая оценить степень воздействия и срочность инцидентов. Эта информация также может быть получена от пользователя, но в этом случае она, возможно, будет менее полной и достаточно субъективной, что приведет к увеличению времени разрешения инцидентов.
- База знаний¹. Например, актуальная база данных по проблемам/известным ошибкам, описывающая способ распознавания инцидентов, имеющиеся решения и обходные пути. Она также может включать аналогичные базы знаний от поставщиков.
- Соответствующую автоматизированную систему регистрации, отслеживания и мониторинга инцидентов.

Дополнительно необходимо тесное взаимодействие с Процессом Управления Уровнем Сервисов (Услуг) для определения требуемых приоритетов и времени разрешения инцидентов.

4.5.2. Показатели эффективности²

Для оценки производительности процесса необходимо четко определить контрольные параметры и измеряемые оценки, часто называемые показателями эффективности. Отчет по этим показателям производится регулярно, например раз в неделю, чтобы получить картину изменений, по которой можно было бы определить тенденции. Примерами таких параметров являются:

- общее количество инцидентов;
- среднее время разрешения инцидентов;
- среднее время разрешения инцидентов по приоритетам;
- среднее число инцидентов, разрешенных в рамках соглашений (SLA);
- процент инцидентов, разрешенных первой линией поддержки (без направления в другие группы);
- средняя стоимость поддержки на инцидент;
- число решенных инцидентов на одно рабочее место или на одного сотрудника службы Service Desk;
- инциденты, решенные без посещения пользователя (удаленно);
- число (или процент) инцидентов с первоначально некорректной классификацией;
- число (или процент) инцидентов, неправильно распределенных в группы поддержки.

4.5.3. Функции и роли

Реализация процессов проходит в горизонтальной плоскости через иерархическую структуру организации. Это возможно только при четком определении ответственности и полномочий, связанных с реализацией процессов. Для повышения гибкости может быть использован ролевой подход (т.е. определение ролей). В небольших организациях или в целях снижения общих расходов возможно комбинирование ролей, например, совмещение ролей Руководителя Процессов Управления Изменениями и Управления Конфигурациями.

Руководитель Процесса Управления Инцидентами

Во многих организациях роль Руководителя Управления Инцидентами играет менеджер Службы Service Desk. В сферу ответственности Руководителя Процесса Управления Инцидентами включается следующее:

- мониторинг эффективности и рациональности работы³ процесса;
- контроль работы групп поддержки;

¹ Knowledge Base.

² Performance indicators.

³ Effectiveness and efficiency.

- составление рекомендаций по совершенствованию работы процесса;
- развитие и сопровождение системы Управления Инцидентами.

Персонал групп поддержки

- Первая линия поддержки несет ответственность за регистрацию, классификацию, сопоставление (привязку), распределение по группам поддержки, разрешение и закрытие инцидентов.
- Остальные группы поддержки, прежде всего, принимают участие в расследовании, диагностике и разрешении инцидентов в рамках установленных приоритетов.

4.6. Затраты и проблемы

4.6.1. Затраты

Затраты, связанные с Управлением Инцидентами, включают первоначальные затраты на внедрен: (например, расходы на разработку процесса, обучение и инструктаж персонала), выбор и закуп; инструментальных средств¹ поддержки процесса. Выбор инструментальных средств может занять значительное количество времени. Кроме того, существуют операционные расходы, связанные с оплатой работы персонала и использованием инструментальных средств. Эти затраты во многом зависят от структуры Управления Инцидентами, диапазона видов деятельности, включенных в процесс, сфер ответственности и числа подразделений.

4.6.2. Проблемы

При внедрении Управления Инцидентами могут возникнуть следующие проблемы:

- **Пользователи и ИТ-специалисты работают в обход процедур Управления Инцидентами** — если пользователи будут устранять возникающие ошибки сами или напрямую связываться со специалистами, не следуя установленным процедурам, ИТ-организация не получит информацию о реально предоставляемом Уровне Услуг, числе ошибок и многое другое. Отчеты руководству так» не будут адекватно отражать ситуацию.

- **Перегруженность инцидентами и откладывание «на потом»** — при неожиданном росте количества инцидентов для правильной регистрации может не оказаться достаточно времени, т. к. до окончания ввода информации об инциденте от одного пользователя возникает необходимость обслуживать следующего. В этом случае ввод описания инцидентов может производиться недостаточно точно и процедуры по распределению инцидентов по трупам поддержки не будут выполняться должным образом. В результате решения получаются некачественными и рабочая нагрузка увеличивается еще больше. В случаях, если число открытых инцидентов начинает интенсивно расти процедура экстренного выделения дополнительных ресурсов внутри организации может предотвратить перегрузку персонала.

- **Эскалация** — как известно, в рамках Процесса Управления Инцидентами возможна эскалация инцидентов. Слишком большое число эскалации может оказать отрицательное воздействие на работу специалистов, которые из-за этого отрываются от своей запланированной работы.

- **Отсутствие Каталога Услуг и Соглашений об Уровне Сервисов (SLA)** — если поддерживаемые услуги и продукты недостаточно точно определены, тогда специалистам, вовлеченным в Управление Инцидентами, бывает трудно обоснованно отказать пользователям в помощи.

- **Недостаточная приверженность² процессному подходу со стороны руководства и персонала** - решение инцидентов с помощью процессного подхода обычно требует изменения культуры и более высокого уровня ответственности за свою работу со стороны персонала. Это может вызвать серьезное сопротивление внутри организации. Эффективное Управление Инцидентами требует от сотрудников понимания и реальной приверженности процессному подходу, а не просто участия.

¹ Т. е. программного обеспечения. - Прим. ред.

² Commitment.

Глава 5

Управление Проблемами

5.1. Введение

Как было сказано в предыдущей главе, Процесс Управления Инцидентами начинает действовать с появлением инцидента и прекращает свою работу после исправления ситуации. Это означает, что корневая причина возникновения инцидента не всегда бывает установлена и инцидент может повториться снова.

Для выяснения корневых причин возникновения как существующих, так и потенциальных ошибок в предоставлении услуг, в рамках Процесса Управления Проблемами производится изучение инфраструктуры и имеющихся регистрационных данных, включая базу данных инцидентов. Такие исследования необходимы из-за сложного и распределенного характера инфраструктуры, когда связи между инцидентами не всегда бывают очевидными. Например, причиной проблемы могут стать сразу несколько ошибок, и в то же время несколько проблем могут быть связаны с одной и той же ошибкой. Вначале надо определить причину возникновения проблемы. После того, как корневая причина определена, проблема переходит в разряд известных ошибок и для устранения этой причины можно направить Запрос на Изменение¹. Но даже после этого известные ошибки будут отслеживаться и контролироваться в рамках Процесса Управления Проблемами. Поэтому следует вести регистрацию всех идентифицированных известных ошибок, их симптомов и имеющихся решений.

5.1.1. Определение — «проблема» и «известная ошибка»

На рис 5.1 показаны взаимосвязи между проблемой, известной ошибкой и Запросом на Изменение и даны определения этих терминов.

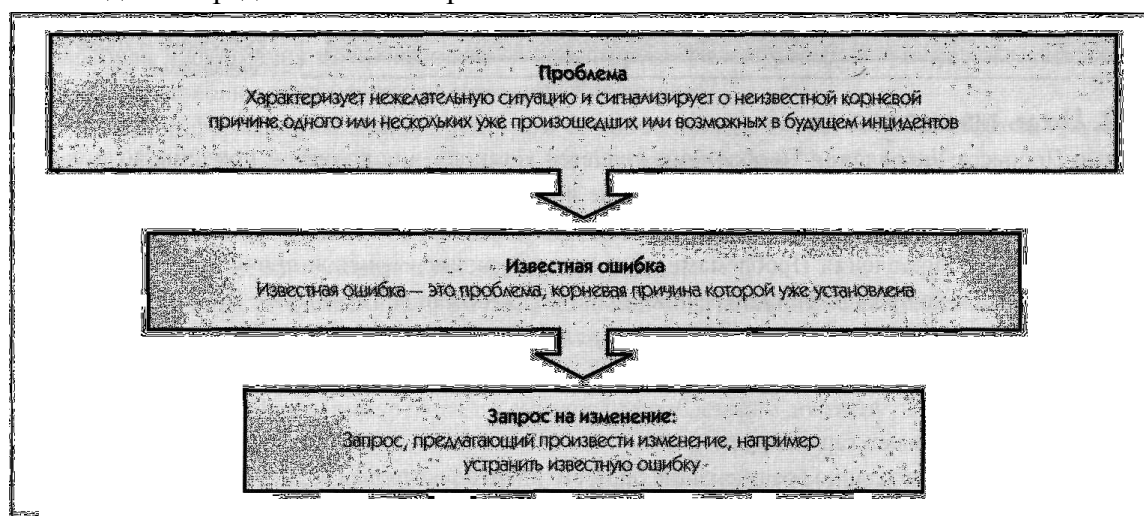


Рис. 5.1. Отношения между проблемами и известными ошибками (источник: OGC)

5.1.2. Взаимоотношения с Процессом Управления Инцидентами

Процесс Управления Проблемами поддерживает Процесс Управления Инцидентами, предоставляя ему обходные решения и быстрые исправления², но при этом не неся прямой ответственности за разрешение инцидента. Управление Инцидентами помогает быстро исправить ошибку любыми доступными средствами, включая обходные решения, в то время как Управление Проблемами занимается поиском причины произошедшего и ее устранением. Инцидент может никогда «не стать» проблемой. Однако кроме самого инцидента, может быть определена связанная с ним проблема. Поэтому работа над проблемой может помочь в разрешении текущего инцидента, если он еще открыт.

¹ Request for Change - RFC

² Quick fixes — быстрые исправления, быстрые решения или «заплатки», т. е. решения, позволяющие быстро устранить инцидент, но не устраняющие ошибку.

На рис. 5.2 показаны отношения между инцидентами, проблемами, известными ошибками и изменениями.

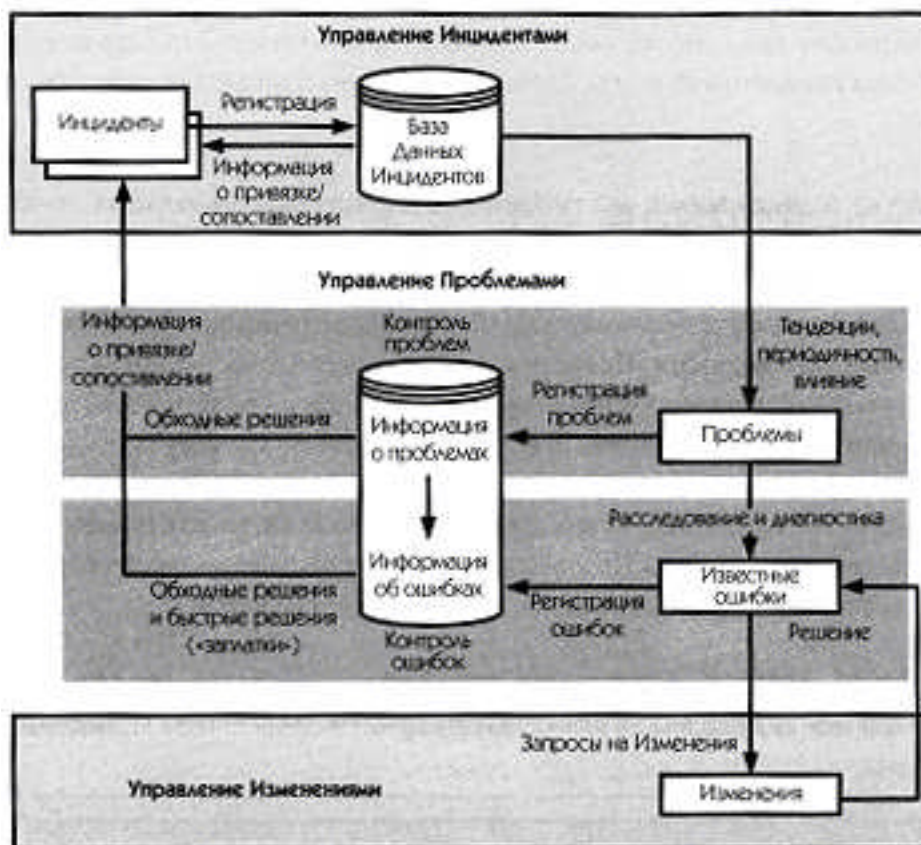


Рис. 5.2. Отношения между Процессами Управления Инцидентами, Управления Проблемами и Управления Изменениями.

5.2. Цель процесса

Целью Процесса Управления Проблемами является установление корневой причины возникновения проблемы и, как следствие, предотвращение инцидентов. Управление Проблемами включает в себя проактивные (упреждающие) и реактивные виды деятельности. Задачей реактивных составляющих Процесса Управления Проблемами является выяснение корневой причины прошлых инцидентов и подготовка предложения по ее ликвидации. Проактивное Управление Проблемами помогает предотвратить инциденты путем определения слабых мест в инфраструктуре и подготовки предложений по ее усовершенствованию.

Управление Проблемами гарантирует, что:

- существующие и регулярно возникающие ошибки¹ идентифицированы, документированы и отслеживаются;
- симптомы ошибок, постоянные или временные решения документируются;
- подаются Запросы на Изменения с целью модификации инфраструктуры;
- предотвращается возникновение новых инцидентов;
- создаются отчеты о качестве инфраструктуры ИТ и самого процесса.

Управление Проблемами позволяет быстро улучшить качество услуг путем значительного сокращения количества инцидентов и уменьшения рабочей нагрузки на ИТ-организацию. Некоторые из преимуществ данного процесса состоят в следующем:

- **Улучшение качества ИТ-услуг и Управления** — результат документирования ошибок и/или их устранения.
- **Повышение производительности труда пользователей** — за счет улучшения качества услуг.

¹ Long-term errors.

- **Повышение производительности труда персонала** — наличие документированных решений проблем позволяет даже менее опытным участникам Процесса Управления Инцидентами разрешать инциденты быстрее и эффективнее.
- **Улучшение репутации ИТ-услуг** — в результате улучшения стабильности услуг заказчики с большим желанием сотрудничают с ИТ-организацией в новых сферах бизнеса.
- **Совершенствование знаний в области Управления, эффективное обучение** — Процесс Управления Проблемами позволяет хранить исторические данные¹, которые используются при определении тенденций и помогают принять меры по предотвращению новых инцидентов. Исторические данные также можно использовать при проведении исследований и диагностирования, а также, при создании Запросов на Изменения.
- **Улучшение регистрации инцидентов** — Управление Проблемами вводит стандарты на регистрацию и классификацию инцидентов с целью эффективного определения проблем и их симптомов. Это также помогает улучшить составление отчетов об инцидентах.
- **Более высокая доля инцидентов, разрешенных на первой линии поддержки** — поскольку Процесс Управления Проблемами разрабатывает решения для ликвидации инцидентов и проблем, а обходные решения можно найти в базе знаний, то первая линия поддержки с большим успехом сама разрешает инциденты.

5.3. Процесс

Входами для Процесса Управления Проблемами являются:

- детальные описания инцидентов;
- обходные решения, найденные Процессом Управления Инцидентами;
- детали конфигурации из Конфигурационной Базы Данных (CMDB);
- подробная информация от производителя используемых в инфраструктуре продуктах, включая известные ошибки в этих продуктах и технические детали;
- подробная информация об инфраструктуре и ее поведении, такая как записи о имеющихся мощностях, замеры производительности, отчеты о соблюдении Уровней Услуг и так далее.

Основными видами деятельности в рамках Процесса Управления Проблемами являются:

- **контроль проблем:** определение и исследование проблем;
- **контроль ошибок:** отслеживание известных ошибок и подача Запросов на Изменения (RFC);
- **проактивное Управление Проблемами:** предотвращение инцидентов путем совершенствования инфраструктуры;
- **предоставление информации:** отчеты по серьезным проблемам и достигнутым результатам.

Выходами процесса являются:

- известные ошибки;
- Запросы на Изменения (RFC);
- новые регистрационные данные о проблемах (обновленные с учетом информации о способах решения и/или обходных решениях);
- закрытые после устранения причины проблемы регистрационные записи;
- информация для руководства.

¹ Historical data.



Рис. 5.3. Управление Проблемами среди других процессов

С Управлением Проблемами связаны следующие процессы:

5.3.1. Управление Инцидентами

Управление Инцидентами является важным партнером Процесса Управления Проблемами. Эффективная регистрация инцидентов важна для успешного Управления Проблемами, так как эта информация используется при идентификации проблемы.

Управление Проблемами поддерживает Процесс Управление Инцидентами. Процесс Управления Проблемами изучает проблемы и, пока не будет найдено решение, Управлению Инцидентами предлагаются обходные решения для работы над инцидентом. После установления причины и определения Известной ошибки, может быть предложено быстрое решение («заплатка»)¹, которое поможет предотвратить возникновение инцидентов на некоторое время или уменьшит их негативные последствия. Управление Проблемами может подать Запрос на Изменение, который приведет к окончательному решению.

Примечание, обходные решения могут создаваться и в Процессе Управления Инцидентами, и в Процессе Управления Проблемами.

5.3.2. Управление Изменениями

Управление Изменениями отвечает за контролируемое проведение изменений, включая Запросы на Изменения для устранения проблем, предложенные Процессом Управления Проблемами. Управление Изменениями несет ответственность за определение степени воздействия изменения и ресурсов, необходимых для его реализации, а также за планирование, согласование и оценку запрашиваемых изменений. Кроме того, Управление Изменениями информирует Процесс Управления Проблемами

О ходе работ и о завершении корректирующих изменений. Оценка этим изменениям дается совместно с Процессом Управления Проблемами. Итогом работы является Анализ результатов внедрения², после которого в рамках полпроцесса Контроля ошибок может быть закрыта известная ошибка, а также относящиеся к ней (открытые) инциденты.

5.3.3 Управление Конфигурациями

Процесс Управления Конфигурациями предоставляет важную информацию об элементах инфраструктуры, документации, конфигурации программного и аппаратного обеспечения, ИТ-

¹ Quick Fix.

² Post Implementation Review — PIR.

сервисах и других отношениях типа «связан с», «использует» и «является частью». Эти отношения являются исключительно важными для решения проблем.

5.3.4. Управление Доступностью

Процесс Управления Доступностью нацелен на планирование и реализацию согласованных Уровней Доступности. Управление Проблемами оказывает поддержку Управлению Доступностью, определяя и устраняя причины недоступности услуг. Процесс Управления Доступностью направлен на разработку архитектуры и проектирование инфраструктуры, его задача — предупреждать появление проблем и инцидентов путем оптимизации планирования доступности услуг и ее мониторинга.

5.3.5. Управление Мощностями

Управление Мощностями позволяет оптимизировать использование ИТ-ресурсов. Данный процесс предоставляет Управлению Проблемами важную информацию, которую можно использовать для определения проблем. Управление Проблемами оказывает поддержку Управлению Мощностями, устанавливая причины соответствующих проблем и устраняет их.

5.3.6. Управление Уровнем Услуг

Управление Уровнем Услуг включает в себя работы по согласованию и заключению Соглашений о Качестве ИТ-услуг. Управление Уровнем Услуг передает в Процесс Управления Проблемами информацию, которая используется при определении проблем. Процедуры Процесса Управления Проблемами должны поддерживать предоставление услуг в соответствии с согласованными стандартами качества. Эту же роль Управление Проблемами играет в Процессах Управления ИТ-финансами и Управления Непрерывностью ИТ-услуг.

5.4. Виды деятельности 5.4.1. Контроль проблем

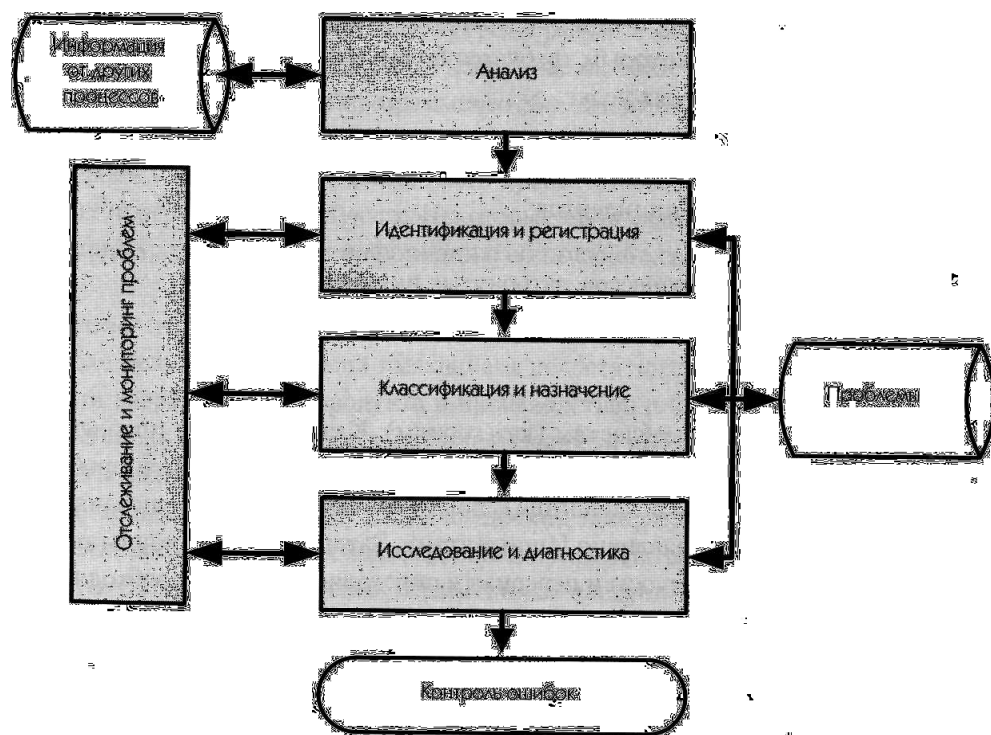


Рис. 5.4. Контроль проблем (источник: OGC)

Целью этого вида деятельности является выявление проблем и изучение их причин. Контроль проблем должен преобразовать проблему в известную ошибку путем диагностирования неизвестной причины ее возникновения. На рис. 5.4 показаны действия, выполняемые в рамках контроля проблемы.

Идентификация и регистрация проблемы

В принципе, любой инцидент, возникший по неизвестной причине, может быть связан с проблемой. На практике это имеет смысл делать только тогда, когда инцидент повторяется, возможно его повторение или если это единичный, но серьезный инцидент.

Деятельность по «идентификации проблем» часто выполняют Координаторы проблем. Однако бывает так, что персонал, изначально не вовлеченный в эту работу, например, специалисты по Управлению Мощностями, тоже может выявлять проблемы. Такие «находки» также следует регистрировать как проблемы.

Регистрационные детали проблем схожи с деталями инцидентов, но в случае проблемы не нужно включать в описание информацию о пользователе и т. д. Однако инциденты, связанные с конкретной проблемой, следует идентифицировать и соответствующим образом регистрировать. Ниже даются примеры случаев, когда могут быть идентифицированы проблемы:

- Анализ инцидентов показывает, что некоторый инцидент повторяется, возникает большое количество инцидентов или возникает негативная тенденция.
- Анализ инфраструктуры позволил определить ее слабые места, где могут произойти новые инциденты (возможно, это проводилось средствами Процессов Управления Доступностью и Управления Мощностями).
- Произошел серьезный инцидент, требующий структурного решения для предотвращения его повторения в будущем.
- Существует угроза срыва Уровня Услуг, согласованного с заказчиком (по показателям производительности, мощности ИТ-средств, затрат и т. д.)
- Нельзя установить связь между новыми инцидентами и уже известной проблемой или ошибкой.
- Нельзя установить связь между зарегистрированными инцидентами и любой из известных проблем или ошибок.

Анализ тенденций позволяет обнаружить области, которым требуется особое внимание. Необходимые для этого дополнительные ресурсы нужно обосновать с позиции издержек и выгод для организации. Например, определить области, которым требуется более действенная поддержка, и понять, насколько они важны для предоставляемых услуг.

Такая оценка может базироваться на «болевом показателе» инцидентов, в котором учитываются:

- издержки, которые несет бизнес из-за инцидентов;
- количество инцидентов;
- количество пользователей и бизнес-процессов, затронутых инцидентами;
- время и затраты на разрешение инцидентов.

Классификация и назначение

Проблемы можно классифицировать по областям (категориям). Классификация проблемы выполняется одновременно с анализом степени ее воздействия, т. е. уровня серьезности проблемы и ее влияния на услуги (срочность и степень воздействия). Вслед за этим проблеме присваивается приоритет, точно так же, как в Процессе Управления Инцидентами. Затем на основе результатов классификации за проблемой закрепляются ресурсы и персонал и определяется время, необходимое для ее решения.

Классификация проблемы включает в себя следующее:

- **Категория:** определение области, например, программное или аппаратное обеспечение;
- **Степень воздействия на бизнес-процесс;**
- **Срочность:** допустимая задержка в решении проблемы;

- **Приоритет:** показатель, объединяющий срочность, степень воздействия, риск и необходимые ресурсы;
- **Статус:** например, проблема, известная ошибка и т. д.

Классификация не является статичной, она может меняться на протяжении жизненного цикла проблемы. Например, наличие обходного решения или быстрого решения поможет снизить срочность проблемы, в то время как новые инциденты могут привести к усилению степени воздействия проблемы.

Расследование и диагностика

Расследование и диагностика являются итеративными фазами процесса, они неоднократно повторяются, каждый раз приближаясь все ближе к намеченному результату. Часто делаются попытки воспроизвести инцидент в условиях тестирования. Для решения проблемы могут потребоваться дополнительные знания, например, для анализа и диагностики проблемы можно привлечь специалистов из группы поддержки.

Проблемы возникают не только из-за программных или технических средств. Они могут быть вызваны ошибками в документации, ошибками персонала или процедурными ошибками, такими как выпуск неправильной версии программного обеспечения. Поэтому желательно включать описания процедур в Конфигурационную Базу Данных и проводить контроль их версий. В то же время многие ошибки связаны с компонентами ИТ-инфраструктуры.

После того как установлена причина проблемы, определены Конфигурационные Единицы или группы единиц, ее вызвавшие, установлена связь между Конфигурационной Единицей и инцидентом (инцидентами), становится возможным определить Известную ошибку. После этого Управление Проблемами продолжит свою работу, выполняя функции контроля ошибок.

Источники ошибок в других средах

В большинстве случаев ошибки выявляются только тогда, когда система находится в реальной рабочей среде. Однако продукты, поступающие из среды разработки (от внешних поставщиков и внутренних разработчиков), также могут содержать известные ошибки (дефекты). Примечание: для компаний-разработчиков среда разработки программного обеспечения является их промышленной средой. Обычно разработчики и поставщики должны сообщать, какие ошибки содержатся в каждой конкретной версии. Отраслевые издания часто предоставляют информацию об известных ошибках в популярных программных продуктах. Некоторые производители поставляют свои продукты вместе с базами данных, содержащими информацию об имеющихся в продуктах известных ошибках.

Если известные ошибки в продукте не представляют серьезной опасности или если бизнес настаивает на запуске релиза, несмотря на имеющиеся недостатки, то может быть принято решение об использовании разработанного продукта в производственной среде, но при этом необходимо, чтобы известные ошибки были учтены в рамках деятельности по Контролю ошибок. В этом случае следует организовать взаимодействие с Процессом Управления Инцидентами, чтобы быстро распознавать инциденты, произошедшие в результате внедрения таких продуктов. В случаях необходимости также могут быть предоставлены обходные решения или быстрые исправления. Перед началом внедрения продукта Процессу Управления Изменениями следует принять решение о приемлемости имеющихся известных ошибок. Часто такое решение принимается под давлением, так как пользователи ждут появления новой функциональности.

5.4.2. Контроль ошибок

Деятельность по Контролю ошибок заключается в ведении мониторинга и исправлении известных ошибок до момента их полного устранения (в тех случаях, когда это возможно и целесообразно). Эта задача решается путем подачи Запроса на Изменение (RFC) в Процесс Управления Изменениями и оценки внесенных изменений с помощью Анализа результатов внедрения (PIR). В рамках Контроля ошибок осуществляется деятельность по мониторингу всех

известных ошибок с момента их идентификации и до устранения. К работе по Контролю ошибок привлекаются многие подразделения, как из операционной среды, так и из среды разработки.

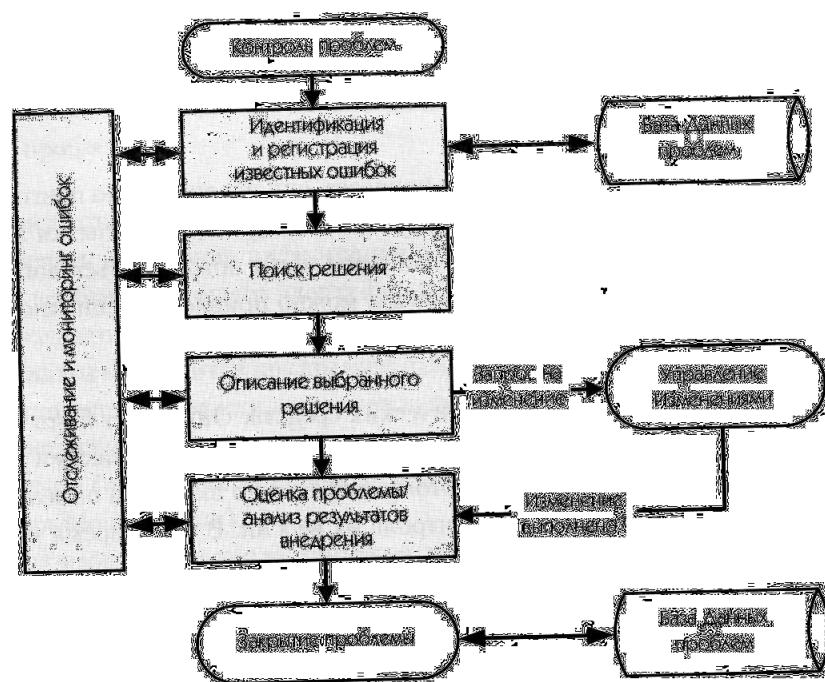


Рис. 5.5. Контроль ошибок
(источник: OGC)

Идентификация и регистрация ошибок

После определения причины проблемы и связанной с ней Конфигурационной Единицы, проблеме присваивается статус «Известной ошибки» и начинается деятельность по Контролю ошибок. Во многих случаях уже имеется обходное решение для проблемы, даже если ошибка найдена самими разработчиками. Но в некоторых случаях обходное решение нужно найти, а затем передать его в Процесс Управления Инцидентами, если там еще имеются открытые инциденты. Это обходное решение также можно использовать во время сопоставления инцидентов¹.

Поиск решения

Персонал, участвующий в Управлении Проблемами, определяет, что необходимо сделать для разрешения известной ошибки. Специалисты сравнивают различные решения, принимая во внимание Соглашения об Уровне Услуг (SLA), возможные издержки и выгоды. Они определяют степень влияния и срочность Запросов на Изменения. Все работы по выработке решения должны быть зафиксированы в системе, у персонала должны быть средства для мониторинга проблем и определения их статуса.

Срочное исправление

Во время работы может потребоваться разрешение на выполнение срочного исправления, если известная ошибка ведет к возникновению серьезных инцидентов. Если для выполнения экстренного или быстрого исправления нужно модифицировать инфраструктуру, то вначале следует подать Запрос на Изменение. Если ситуация очень серьезная и задержка решения недопустима, то приводится в действие процедура проведения срочных изменений.

Определение окончательного решения

На предыдущих этапах происходит выбор оптимального решения. Однако может быть принято решение не исправлять известную ошибку, например, по причине экономической нецелесообразности.

¹ Т. е. во время сопоставления новых инцидентов с известными ошибками. — Прим. ред.

Например, компания, у которой есть проблемы с собственными разработками системы ERP, приостанавливает любые исправления кодов существующей системы, так как принято стратегическое решение о переходе на SAP к концу года. В этом и других аналогичных случаях полученные преимущества не перевешивают затраты на исправления. Или же в другом случае степень воздействия ошибки может оказаться приемлемой, инцидент может оказаться легким для исправления или же вероятность его повторения невысока. В некоторых случаях исправление известной ошибки вообще невозможно без приложения усилий, несоизмеренных проблеме. Но какое бы решение не было принято, оно должно быть отражено в системе, чтобы его можно было использовать в Процессе Управления Инцидентами.

После окончания этапа выбора существует достаточно информации для подачи Запроса на Изменение. Далее исправление известной ошибки будет произведено в рамках Процесса Управления Изменениями.

Анализ результатов внедрения¹ (PIR)

Изменение, предназначенное для устранения известной ошибки, должно быть рассмотрено при анализе результатов внедрения до закрытия проблемы. Если изменение дало ожидаемый результат, проблема может быть закрыта, и в базе данных о проблемах ее статус будет изменен на статус «решена». Управление Инцидентами будет проинформировано об этом и инциденты, связанные с этой проблемой, тоже могут быть закрыты.

Примечание: Во многих организациях процесс реализован таким образом, что проблема закрывается только после того, как будут закрыты связанные с ней инциденты (и закрытие проверено заказчиком), иначе если инциденты не удастся закрыть, то проблему будет необходимо открывать снова.

Отслеживание и мониторинг

Данная задача предполагает выполнение мониторинга хода работ по разрешению проблем и известных ошибок на всех этапах Контроля проблем и Контроля ошибок. Цели состоят в следующем:

Определить, изменилась ли степень влияния или срочность проблемы, и на основании этого производить корректировку приоритета проблемы.

Вести мониторинг процесса выработки и реализации решения и контролировать правильность исполнения Запроса на Изменение. По этой причине Управление Изменениями регулярно передает информацию о состоянии Запросов на Изменение в Контроль ошибок.

Предоставление информации

В течение всего процесса информация об обходных решениях и быстрых исправлениях передается в Управление Инцидентами. Пользователи также могут информироваться об этом. Хотя данные предоставляет Процесс Управления Проблемами, их распространением занимается Служба Service Desk. Управление Проблемами использует Конфигурационную Базу Данных, а также Соглашения об Уровне Услуг, для уточнения, какую информацию и кому следует предоставлять.

5.4.3. Проактивное Управление Проблемами

Проактивное Управление Проблемами (т. е. предупреждающее появление проблемы) имеет дело с вопросами качества инфраструктуры. Оно сосредоточено на анализе тенденций и выявлении потенциальных угроз инцидентов до того, как они произойдут. Это достигается путем изучения слабых и перегруженных компонентов инфраструктуры. Если таких областей несколько, тогда делается попытка предотвращения появления в них ошибок, которые наблюдались в других местах. Слабые места инфраструктуры должны быть выявлены и изучены.

5.5. Управление Процессом

¹ Post Implementation Review - PIR.

5.5.1. Отчеты об Управлении и Ключевые показатели эффективности

Успешное Управление Проблемами проявляется в:

- сокращении количества инцидентов в результате разрешения проблем;
- сокращении времени, требуемом для разрешения проблем;
- уменьшении других затрат, связанных с разрешением проблем.

Параметры процесса также могут быть включены в отчеты для внутренних целей Управления, для оценки и контроля эффективности Управления Проблемами.

Отчеты об Управлении Проблемами могут быть достаточно объемными и охватывать следующие аспекты:

- **Отчеты о времени исполнения:** разделенные на Контроль проблем, Контроль ошибок и проактивное Управление Проблемами, а также разделенные между группой поддержки и поставщиком.

- **Качество продукта:** детальная информация об инциденте, проблеме и известной ошибке может помочь выявлению продуктов, подверженных частым ошибкам, и установлению, могут ли поставщики в этом плане принять на себя соответствующие контрактные обязательства.

- **Эффективность¹ Процесса Управления Проблемами:** точное количество инцидентов до и после решения проблемы, зарегистрированные проблемы, количество поданных Запросов на Изменения и решенных известных ошибок.

- **Баланс между реактивным и проактивным Управлением Проблемами:** увеличение объема проактивного Управления Проблемами по сравнению с простым реагированием на инциденты свидетельствует о большей зрелости процесса.

- **Качество разработанных продуктов:** продукты, переданные от разработчиков, должны иметь высокое качество, иначе они могут создать новые проблемы. Для мониторинга качества важны отчеты о новых продуктах и имеющихся в них известных ошибках.

- **Статус и план работ по открытым проблемам:** итоговый отчет о том, что было сделано и что будет сделано для разрешения наиболее серьезных проблем, включая запланированные Запросы на Изменения, необходимое время и ресурсы.

- **Предложения по улучшению Процесса Управления Проблемами:** если отчетная информация по перечисленным выше аспектам указывает на то, что процесс не соответствует Плану обеспечения качества услуг, нужно предлагать меры по совершенствованию процедур регистрации, расследования проблем, выполнения проактивных действий, а также для выделения дополнительных ресурсов. В планировании и улучшении процесса могут помочь регулярные аудиторские проверки.

Содержание отчетов зависит от сферы действия Процесса Управления Проблемами. Если в сферу действия процесса попадают продукты из среды разработки, то Управление Проблемами может определять известные ошибки и вести их мониторинг даже на этапе разработки программного обеспечения.

5.5.2. Критические факторы успеха

Успешное Управление Проблемами зависит от следующих факторов:

- Эффективная автоматизированная регистрация инцидентов и эффективный контроль за состоянием инфраструктуры.

- Наличие реалистичных целей и максимальное использование знаний и опыта персонала, например, наличие соглашения о возможности привлечения специалистов в обусловленное время и резервировании достаточного времени на их работу по исследованию корневых причин проблем.

- Эффективность взаимодействия Управления Проблемами и Управления Инцидентами. При распределении заданий и работ нужно учитывать конфликт интересов этих двух процессов: «тушение пожара» в рамках Управления Инцидентами и необходимость выяснения корневых причин в рамках Управления Проблемами.

¹ Effectiveness.

5.5.3. функции и роли

Работа процессов происходит в горизонтальной плоскости, проходя через различные иерархические (вертикальные) подразделения организации и функциональные обязанности в рамках отделов. Эффективная работа возможна только при четком определении ответственности и полномочий, связанных с реализацией процессов. Для повышения гибкости может быть использован ролевой подход. Если организация небольшая или имеются соответствующие экономические ограничения, то возможно комбинирование ролей, например, Руководителя Процессы Управления Проблемами и Процессы Управления Уровнем Сервиса. Последний пункт в разделе 5.5.2 объясняет, почему многие организации избегают объединения ролей руководителя службы Service Desk/Управления Инцидентами и Руководителя Процессы Управления Проблемами.

Руководитель Процессы Управления Проблемами

Руководитель Процессы несет ответственность за такие виды деятельности по Управлению Проблемами, как:

- разработка и поддержка подпроцессов Контроля проблем и Контроля ошибок;
- оценка эффективности и рациональности¹ работ по Контролю проблем и Контролю ошибок;
- предоставление Управленческой Информации;
- Управление Персоналом, участвующим в Процессы Управления Проблемами;
- обеспечение необходимых ресурсов;
- разработка и совершенствование систем Контроля Проблем и Контроля Ошибок;
- анализ работы и оценка эффективности проактивного Управления Проблемами.

Роли поддержки деятельности по Управлению Проблемами

Ответственность персонала, выполняющего роли по решению проблем:

- Реактивное Управление:
 - выявление и регистрация проблемы путем анализа информации об инцидентах;
 - изучение проблем на основе их приоритетности;
 - подача Запросов на Изменение;
 - мониторинг устранения ошибок;
 - подготовка рекомендаций по обходным решениям и быстрым исправлениям для Управления Инцидентами.
- Проактивное Управление:
 - определение тенденций;
 - подача Запросов на Изменения;
 - предотвращение распространения проблем на другие системы.

5.6. Затраты и проблемы

5.6.1. Затраты

В дополнение к расходам на средства поддержки и диагностики необходимо учитывать расходы на персонал. Кроме затрат на содержание собственного ИТ-персонала, участвующего в Управлении Проблемами, есть еще расходы на специалистов, привлеченных из сторонних организаций. Однако следует заметить, что все связанные с этим расходы обычно успешно окупаются через получаемые преимущества.

5.6.2. Проблемы

¹ Effectiveness and efficiency.

На следующие вопросы следует обратить внимание при реализации Процесса Управления Проблемами и, по возможности, их избежать:

- **Плохая связь между Процессами Управления Инцидентами и Управления Проблемами:** если связь между работами над инцидентами, проблемами и известными ошибками неадекватна, Процесс Управления Инцидентами не будет знать об обходных решениях для проблем, а Процессу Управления Проблемами будет трудно выполнять оценку и мониторинг проблем. В результате этого будет существовать меньше доступной информации об инфраструктуре и данных о предыстории проблем. Поэтому успешное Управление Проблемами во многом зависит от этого взаимодействия.

- **Недостаточно полная передача информации об известных ошибках из среды разработки в реальную рабочую среду:** информация о программной и технической инфраструктуре, передаваемая в промышленную среду, должна дополняться подробной информацией об известных ошибках. Передача такой информации при развертывании системы позволяет сэкономить время, затрачиваемое на поиски уже известных ошибок. Поэтому должен существовать эффективный обмен данными между двумя системами регистрации проблем (в тестовой и промышленной среде) или должна быть создана единая система.

- **Отсутствие понимания важности процесса:** если существовавший ранее подход был неформальным, может возникнуть сопротивление четкому подходу к Управлению Проблемами, особенно в плане документирования и ведения записей. По этой причине сотрудники, участвующие в Управлении Проблемами, должны быть своевременно информированы о разработке и реализации процесса.

Глава 6.

Управление Конфигурациями

6.1. Введение

В каждой ИТ-организации имеется информация об ИТ-инфраструктуре. Она чаще всего появляется после реализации крупных проектов, которые обычно завершаются проведением аудита и анализом результатов. Главным в работе с такой информацией является поддержание ее в актуальном состоянии. Процесс Управления Конфигурациями помогает получать достоверную и актуальную информацию об ИТ-инфраструктуре. Важным в этой информации является то, что в нее входят данные не только о конкретных единицах конфигурации (Конфигурационных Единицах¹ или CI), но и о том, как они связаны друг с другом. Взаимоотношения и взаимосвязи между Конфигурационными Единицами составляют основу для анализа степени воздействия инцидентов, проблем, изменений и т. д. на ИТ-инфраструктуру. Процесс Управления Конфигурациями проверяет, правильно ли регистрируются изменения в ИТ-инфраструктуре, включая взаимоотношения между Конфигурационными Единицами (CI), и ведет мониторинг статуса ИТ-компонентов чтобы гарантировать наличие точной информации о версиях существующих Конфигурационных Единиц (CIs).

В случае если Управление Конфигурациями реализовано эффективно, то этот процесс может дать информацию о следующем:

- **Финансовая информация и политика компании в отношении продуктов**

- Какие ИТ-компоненты используются в настоящее время по каждой модели (версии) и на протяжении какого времени?
- Какие тенденции существуют в разных группах продуктов?
- Какова текущая и остаточная стоимость ИТ-компонентов?
- Какие ИТ-компоненты нужно выводить из операционной среды и какие требуют модернизации?
- Сколько будет стоить замена определенных компонентов?
- Какие имеются лицензии и достаточно ли их?
- Какие контракты на сопровождение следует пересмотреть?
- Какова степень стандартизации инфраструктуры?

- **Выявление неисправностей и оценка результатов**

- Какие ИТ-компоненты необходимы для поддержки процесса восстановления в случае чрезвычайной ситуации?
- Будет ли работать план восстановления на случай чрезвычайных обстоятельств, если была изменена Конфигурация Инфраструктуры?
- Какие ИТ-компоненты будут затронуты при развертывании новых сервисов?
- Как оборудование подключено к сети?
- Какие программные модули входят в каждый из комплектов программного обеспечения?
- Какие ИТ-компоненты затрагиваются изменениями?
- Какие Запросы на Изменения (RFC) конкретных ИТ-компонентов находятся на рассмотрении и какие инциденты и проблемы произошли в прошлом и сейчас продолжают оставаться актуальными?
- Какие ИТ-компоненты вызывают известные ошибки?

¹ Configuration items — CI.

- Какие ИТ-компоненты были закуплены у конкретного поставщика в течение определённого периода?

▪ **Предоставление услуг и выставление счетов**

- Какие Конфигурации ИТ-компонентов являются существенными для определенных услуг?

- Какие ИТ-компоненты используются в том или ином месте и кем?

- Какие стандартные ИТ-компоненты может заказать пользователь и какие из них поддерживаются (каталог продуктов)?

6.1.1. Основные понятия

По терминологии процесса Управления Конфигурациями ИТ-компоненты и предоставляемые на их основе услуги называются Конфигурационными Единицами (CI). Каждый ИТ-компонент, чье наличие и версия зарегистрированы, является Конфигурационной Единицей. Как видно из рис. 6.1, Конфигурационными Единицами могут быть технические средства, все виды программного обеспечения, активные и пассивные сетевые элементы, серверы, системные блоки, документация, процедуры, услуги и все другие ИТ-компоненты, контролируемые ИТ-организацией.

Если Управление Конфигурациями применено к информационным системам, а не только к информационным технологиям, то Конфигурационная База Данных¹ (CMDB) может хранить и управлять детальной информацией о пользователях, персонале ИТ-организации и бизнес-структурах. Эти Конфигурационные Единицы также попадают под действие процесса Управления Изменениями, например, при найме и увольнении работников.

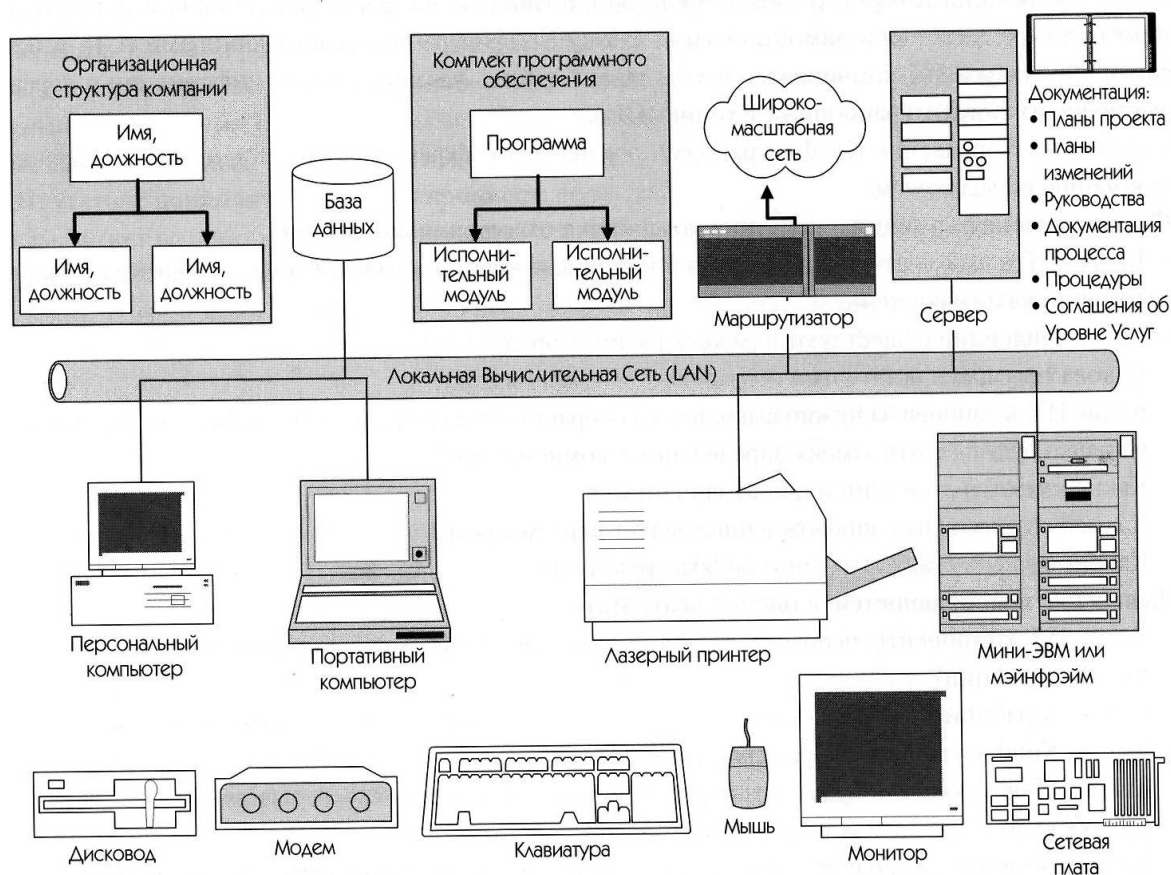


Рис.6.1. Конфигурационные Единицы

Все Конфигурационные Единицы должны быть включены в Конфигурационную Базу Данных (CMDB), которая отслеживает все ИТ-компоненты и взаимоотношения между ними. В самой примитивной форме Конфигурационная База Данных представляет собой набор бумажных форм или электронных таблиц.

¹ Configuration Management Data Base - CMDB.

Разработчики часто используют нечто подобное Конфигурационной Базе Данных для контроля версий всех программных модулей. Некоторые платформы предоставляют такой вид контроля. Конфигурационная База Данных может состоять из нескольких физически отдельных баз данных, которые вместе составляют единое логическое целое. Рекомендуется оптимально интегрировать различные источники Конфигурационных Данных.

Не следует путать Конфигурационную Базу Данных со складскими или инвентаризационными базами данных. Такие программы предоставляют только ограниченную информацию о действующем аппаратном и программном обеспечении, сетевых компонентах и компонентах среды. Кроме того, Конфигурационная База Данных (CMDB) демонстрирует, какой должна быть инфраструктура, если все идет по плану (см. также Управление Изменениями), включая документацию. Данные в базе CMDB фактически представляют авторизованную Конфигурацию Инфраструктуры. Список расхождений (дельта) между бухгалтерскими и Конфигурационными Базами Данных является источником ценной информации. Управление Конфигурациями не следует путать с Управлением Активами.

- **Управление Активами** — это бухгалтерский процесс мониторинга амортизации активов, чья закупочная цена превышает определенную величину. Мониторинг ведется путем учета закупочных цен, амортизации, месторасположения активов. Эффективно работающая система Управления Активами может послужить основой для системы Управления Конфигурациями.

- **Управление Конфигурациями** идет дальше, учитывая также информацию о взаимоотношениях между Конфигурационными Единицами и решая задачу стандартизации и авторизации единиц CI. Управление Конфигурациями также контролирует информацию о статусе ИТ-компонентов, их расположении, произведенных в них изменениях и т. д.

6.2. Цель процесса

Цель процесса Управления Конфигурациями — содействие в Управлении Значимостью¹ ИТ-услуг (сочетание требований заказчика, качества и затрат) путем поддержки логической модели ИТ-инфраструктуры и ИТ-услуг и предоставления информации о них другим бизнес-процессам. Это достигается посредством идентификации, мониторинга, контроля и предоставления информации о Конфигурационных Единицах и их версиях. Задачами данного процесса являются:

- точная регистрация детальной информации об ИТ-компонентах и услугах, предоставляемых организацией;
- предоставление точной информации и документации для поддержки других процессов сервис-менеджмента.

6.2.1. Преимущества использования процесса

Управление Конфигурациями содействует рентабельному предоставлению высококачественных ИТ-услуг с помощью:

- **Управления ИТ-компонентами** — ИТ-компоненты являются крайне важным элементом при предоставлении ИТ-услуг. Каждая услуга включает одну или несколько Конфигурационных Единиц, и процесс Управления Конфигурациями контролирует, что происходит с этими единицами.

- **Повышения качества коммерческих услуг** — процесс Управления Конфигурациями помогает в обработке изменений, выявлении и разрешении проблем и поддержке пользователей. Это приводит к сокращению количества ошибок и, как следствие, к уменьшению расходов.

- **Эффективного разрешения проблем** — Управление Конфигурациями помогает в определении Конфигурационных Единиц, затронутых проблемой, и контролирует модификацию и замену этих элементов. Данный процесс также предоставляет информацию о тенденциях, которая является также входной информацией для Управления Проблемами.

- **Более быстрой обработки изменений** — Управление Конфигурациями помогает в проведении более быстрого и точного анализа степени влияния, поэтому изменения могут быть реализованы быстрее и эффективнее.

¹ Economic value.

- **Лучшего контроля аппаратного и программного обеспечения** — распространение пакетов программ по возможности нужно объединять с установкой (распространением) аппаратного обеспечения и проведением предварительного тестирования. Конфигурационную Базу Данных и Базисные Конфигурации (т. е. мгновенные «фотографии» состояния инфраструктуры) можно использовать для разработки плана тестирования и распространения конкретным группам пользователей. В базе также содержится информация о проверенных версиях программного обеспечения, которые можно использовать при проведении изменений в случае необходимости возврата в исходное состояние.

- **Улучшенной безопасности** — Управление Версиями дает информацию об авторизованных изменениях в **Конфигурационных** Единицах и использовании различных модификаций программного обеспечения. Такая информация из Конфигурационной Базы Данных также помогает в мониторинге лицензий.

- **Соблюдения требований закона** — незаконные копии будут выявляться при сравнении результатов аудиторской проверки с Конфигурационной Базой Данных. Это может принести дополнительную пользу организации, т. к. незаконные версии могут содержать вирусы, а процесс Управления Конфигурациями может защитить организацию от их проникновения. В некоторых организациях не так легко помешать персоналу использовать незаконное и потенциально зараженное программное обеспечение, тем не менее тот факт, что такие версии могут быть обнаружены с помощью процесса Управления Конфигурациями, Конфигурационной Базы Данных и аудиторских проверок и что по результатам проверок будут приняты дисциплинарные меры, послужат предостережением персоналу. На нарушение правил персонал обычно толкает мысль, что об этом никто не узнает.

- **Более точного планирования расходов** — Конфигурационная База Данных предоставляет информацию о затратах на сопровождение и контракты, лицензии и продукцию с истекшим сроком эксплуатации.

- **Лучшей поддержки процессов Управления Доступностью и Управления Мощностями** — эти процессы в части планирования и анализа услуг зависят от правильной детальной информации о Конфигурациях.

- **Крепкого надежного фундамента для Управления Непрерывностью ИТ-услуг** - Конфигурационная База Данных, если имеется ее резервная копия в надежном месте, может играть важную роль в восстановлении услуг в случае чрезвычайных обстоятельств. База также помогает в определении Конфигурационных Единиц, необходимых для такого восстановления, включая соответствующие процедуры и руководства, если они входят в состав базы.

- **Определение скрытых затрат** — большая часть персонала ведет учетные записи о той части инфраструктуры, за которую они отвечают. Поскольку такая информация может собираться разными людьми и с разными целями, то в ней могут наблюдаться частичные совпадения. Дублирование и противоречивость в данных всегда влекут за собой дополнительные затраты и связаны с риском.

6.3. Процесс

Входом для процесса Управления Конфигурациями является информация об изменениях и информация из процесса Управления Закупками, а выходом — отчеты для других процессов и ИТ-руководства. Есть еще другой выход, когда Управление Конфигурациями предоставляет данные из Конфигурационной Базы Данных другим процессам, необходимые им для выполнения своих задач.

Процесс Управления Конфигурациями связан с многими другими процессами.

6.3.1. Управление Инцидентами

Процессу Управления Инцидентами необходима информация о всей инфраструктуре. При регистрации инцидентов процессу нужен доступ к информации о Конфигурационных Единицах, например, для определения расположения единицы и ее владельца, для уточнения связи этой единицы с проблемой или известной ошибкой, уже имеющей обходное решение, для какого

заказчика или услуги единица предназначена и каким Соглашением об Уровне Услуг (SLA) регулируется.

6.3.2. Управление Проблемами

Процессу Управления Проблемами нужна информация об инфраструктуре со всеми ее сложными связями и взаимоотношениями. У процесса должны быть возможности для привязки проблем или известных ошибок к Конфигурационным Единицам и для использования информации из Конфигурационной Базы Данных для анализа инцидентов и проблем. Путем сравнения фактической Конфигурации Инфраструктуры с Авторизованной Конфигурацией, хранящейся в базе данных, можно выявить возможные отклонения и дефекты в инфраструктуре.

6.3.3. Управление Изменениями

Процесс Управления Изменениями использует Конфигурационную Базу Данных для оценки степени воздействия планируемых изменений. Данный процесс авторизует проведение изменений, и эти изменения должны быть связаны с соответствующими Конфигурационными Единицами. Управление Изменениями несет ответственность за регистрацию Запросов на Изменения и предоставляет важную входную информацию для обновления Конфигурационной Базы Данных.

6.3.4. Управление Релизами

Процесс Управления Релизами дает информацию о планах выпуска релизов и их версиях, например, о плановых датах основных и второстепенных релизов, а также о произведенных изменениях. Перед выполнением изменения процесс запрашивает информацию о Конфигурационной Единице, например, статус CI, ее расположение, исходный код и т. д.

6.3.5. Управление Уровнем Услуг

Процессу Управления Уровнем Услуг нужна информация о характеристиках услуг и взаимоотношениях между услугами и лежащей в их основе инфраструктурой. Данные из Соглашений об Уровне Услуги в качестве атрибутов могут храниться в Конфигурационной Базе Данных вместе с другой информацией о Конфигурационных Единицах. Данные об Уровне Сервиса (например, «золотой», «серебряный», «бронзовый») записываются для соответствующей сервисной Конфигурационной Единицы или CI для используемого программного или технического компонента.

6.3.6. Управление Финансами

Процессу Управления Финансами необходима информация об использовании услуг, например, у кого имеется в распоряжении РС. Процесс объединяет эту информацию с данными из Соглашений об Уровне Услуг (SLA) для определения цены. Данный процесс также ведет мониторинг инвестиций и стоимости ИТ-компонентов (Управление Активами).

6.3.7. Управление Доступностью

Процесс Управления Доступностью использует Конфигурационную Базу Данных для определения Конфигурационных Единиц, задействованных в услуге, для составления плана изменений и для выявления слабых мест, например, с помощью методики CFIA (Component Failure Impact Analysis — анализ влияния сбоев компонентов на предоставление сервиса). Доступность услуги (цепь компонентов инфраструктуры) определяется тем, насколько надежным является самый слабый компонент (звено цепочки). Процесс Управления Конфигурациями предоставляет информацию о составе цепочки, а также о каждом ее звене.

6.3.8. Управление Непрерывностью ИТ-услуг

Процесс Управления Непрерывностью ИТ-услуг использует стандартные Конфигурации из Конфигурационной Базы Данных (Базисные Конфигурации) для формулирования требований к

восстановлению услуг в случае возникновения чрезвычайных обстоятельств и проверяет наличие этих Конфигураций на запасной территории.

6.3.9. Управление Мощностями

Процесс Управления Мощностями использует данные из Конфигурационной Базы Данных для оптимизации ИТ-инфраструктуры, распределения рабочей нагрузки и разработки плана мощностей.

6.3.10. Виды деятельности

Хотя процесс Управления Конфигурациями, как и другие процессы, представляет собой логическую последовательность действий, в данном процессе они не всегда выполняются строго последовательно. Виды деятельности при Управлении Конфигурациями имеют тенденцию выполняться параллельно. Приведенная ниже последовательность, прежде всего, отражает очередность действий при разработке процесса, а также при обработке и реализации новых информационных требований.

- **Планирование:** определяются стратегия, политика и задачи процесса, анализируется имеющаяся информация, определяются инструментальные средства и ресурсы, создаются интерфейсы с другими процессами, проектами, поставщиками и т. д.

- **Идентификация:** формируется процесс поддержки базы данных в актуальном состоянии. В этот этап входит разработка модели данных для регистрации всех ИТ-компонентов инфраструктуры, взаимоотношений между ними и информации о владельце этих компонентов или лица, ответственного за них, статусе единиц, а также об имеющейся документации. Также должны быть разработаны процедуры создания новых Конфигурационных Единиц и для изменения уже существующих. Поскольку потребности в информации постоянно меняются, определение состава данных о Конфигурации также меняется.

- **Контроль:** контроль обеспечивает актуальное состояние Конфигурационной Базы Данных путем принятия, регистрации и мониторинга авторизованных и идентифицированных Конфигурационных Единиц. Наличие контроля гарантирует, что ни одна Конфигурационная Единица не будет добавлена, изменена, заменена или удалена без соответствующего документа, например, утвержденного Запроса на Изменение или скорректированной спецификации.

- **Мониторинг статуса:** хранение текущей информации и истории статуса Конфигурационной Единицы на протяжении ее жизненного цикла. С помощью мониторинга статуса можно отследить, как меняется статус единицы, например «в разработке», «в тестировании», «в наличии», «в использовании», «выведено из рабочей среды».

- **Верификация:** верификация Конфигурационной Базы Данных путем аудита ИТ-инфраструктуры на наличие в ней зарегистрированных Конфигурационных Единиц и правильности регистрационных записей.

- **Отчетность:** предоставление информации в другие процессы и подготовка отчетов об использовании Конфигурационных Единиц, тенденциях и т. д.

Ниже дается подробное описание этих действий.

6.4. Виды деятельности

6.4.1. Планирование

Задачи процесса Управления Конфигурациями, сфера его действия, а также приоритеты должны определяться в рамках Сервис-менеджмента и обязаны соответствовать бизнес-целям организации. Соответствующие этапы в реализации Управления Конфигурациями выходят за рамки данной книги

6.4.2. Идентификация

Идентификация связана с определением и поддержкой соглашений о присвоении имен и нумерации версий физических компонентов инфраструктуры, взаимоотношений между ними и

атрибутов. Базисные Конфигурации Аппаратного Обеспечения, используемого в настоящий момент и в будущем описываются в форме специальных групп Конфигурационных Единиц (кластеров CI). Общий вопрос, на который должна дать ответ идентификация ИТ-компонентов состоит в следующем:

Какие услуги и связанные с ними компоненты ИТ-инфраструктуры должны находиться под контролем Сервис-менеджмента и какая информация необходима для этого?

При разработке системы идентификации должны быть приняты решения относительно охвата (границ)¹ процесса и уровня детализации регистрируемой информации. Для каждого параметра (характеристики) следует определить владельца или заинтересованное лицо². Чем больше параметров регистрируется, тем больше усилий потребуются на обновление этой информации. Общий вопрос «Что же регистрировать?» может быть сведен к перечню конкретных вопросов для определения требуемой информации, например:

- Какие ресурсы имеются для сбора и обновления информации?
- Насколько зрелыми являются наши административные и материально-технические (логистические) процессы?
- На каких уровнях организация выполняет инсталляцию, замену, разработку и/или распространение компонентов отдельно от основного компонента?
- Какие виды деятельности, выполняемые сторонними организациями, должны измеряться и контролироваться?
- Какие компоненты могут повлиять на услуги в случае сбоя и какая нужна информация для диагностики этих сбоев?
- Для каких компонентов следует регистрировать статус и его предысторию?
- Какие компоненты используются в организации в различных версиях или вариантах?
- Изменения в каких компонентах могут повлиять на возможности и доступность услуг?
- Какие компоненты являются дорогостоящими и их следует защищать от кражи или утери?
- Какова настоящая и будущая информационная потребность у других процессов?
- Для каких компонентов требуется такая информация, как серийный номер, дата покупки и поставщик, и какая информация необходима для бухгалтерии?
- Какие требования вытекают из условий, закрепленных в Соглашениях об Уровне Услуг?
- Какая информация необходима для выставления счетов заказчикам?
- Насколько реальны наши стремления, не нужна ли корректировка?

Ответы на эти вопросы дают представление об объеме работ, которые необходимо выполнить. Следует принять решение об охвате (ширине, границах) CMDB и уровне ее детализации (глубине). Понятие детализации включает в себя: количество уровней в базе данных, взаимоотношения, подлежащие мониторингу, соглашения о присвоении имен и атрибуты. Все они будут рассмотрены ниже.

Охват (сфера действия, границы)³

При создании Конфигурационной Базы Данных и обновлении модели данных следует определиться, какая часть ИТ-инфраструктуры будет находиться под контролем процесса Управления Конфигурациями. Например, следует ли включать в сферу действия данного процесса такие компоненты, как «электронные органайзеры» (PDA), сетевые копировальные устройства, факсы, клавиатуры и ИТ-персонал, или же они должны находиться за пределами действия процесса? Границы, определенные для процесса Управления Конфигурациями, влияют на границы, в которых, например, процесс Управления Проблемами выполняет диагностирование, на анализ степени

¹ Scope.

² Stakeholder.

³ Scope.

воздействия, проводимый процессом Управления Изменениями, планирование, выполняемое процессом Управления Доступностью и т. д.

Кроме того, работая над границами процесса можно произвести анализ вклада ИТ-услуг в конечную деятельность заказчика или степень воздействия на нее, а также рассмотреть соглашения с пользователями об уровне поддержке и услугах.

Сферу действия процесса можно разделить на области, каждая со своими требованиями и подходом к проектированию. Примерами таких областей могут стать настольные рабочие места, системы передачи данных, файловые сервисы, сервисы печати и прикладного ПО, центральная процессинговая система, базы данных, телефонные услуги. Для разработки каждой области может быть инициирован отдельный проект в соответствующей управленческой среде.

Границы Конфигурационной Базы Данных могут включать аппаратное и программное обеспечение, а также документацию, например, Соглашения об Уровне Услуг (SLAs), процедуры, руководства, технические спецификации, организационные схемы, персонал и планы проектов. Как и другие Конфигурационные Единицы, эти документы физически могут находиться в разных местах, но информация о них находится в базе данных с номерами версий, датами публикаций, именами авторов и т. д. В этом случае процессы Управления Конфигурациями и Управления Изменениями могут контролировать эти характеристики документов.

На рис. 6.3 показаны взаимоотношения между услугами и компонентами Конфигурационной Базы Данных. Отслеживание этих взаимоотношений облегчает определение степени воздействия инцидентов на услуги. Это также позволяет создавать отчет обо всех компонентах, вовлеченных в предоставление сервиса. Такая информация в дальнейшем может быть использована для улучшения услуг. У такой «сервисной» Конфигурационной Единицы могут быть взаимоотношения с другими единицами, такие как договоренности с заказчиком в форме Соглашения об Уровне Услуг. В приведенном примере услуга «В» полностью выходит за границы базы данных. Из рисунка видно, что не все Конфигурационные Единицы, участвующие в услуге «А», входят в сферу действия Конфигурационной Базы Данных (например, находятся в рассматриваемой организации), это означает, что услуга «А» не может полноценно поддерживаться.

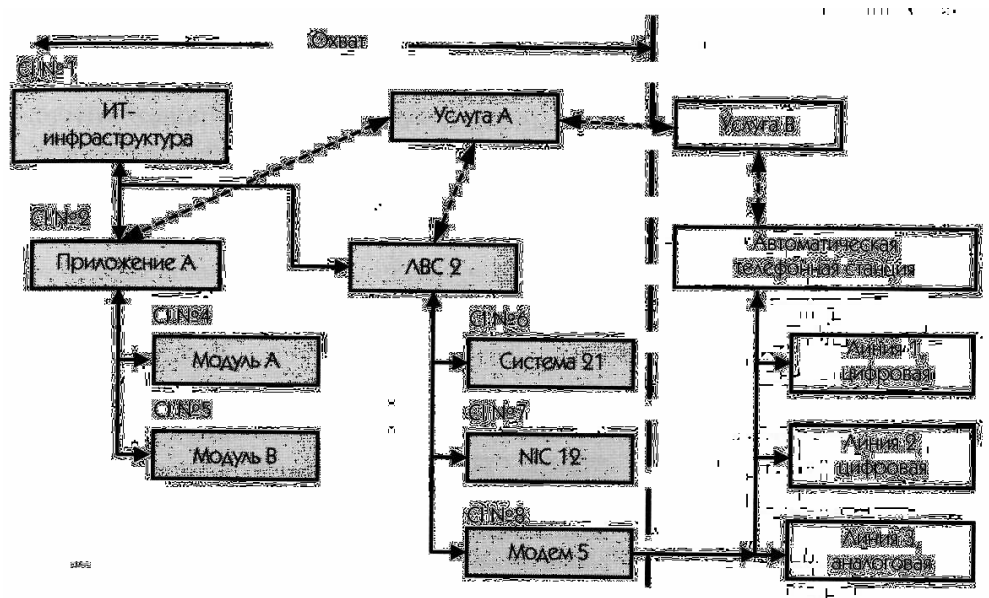


Рис. 6.3. Охват Конфигурационной Базы Данных (источник: OGC)

После определения областей, включенных в сферу действия процесса, возможно определить этапы жизненного цикла Конфигурационных Единиц, которые будут содержаться в CMDB. Будут ли единицы со статусом «в разработке» или «заказана» включены в базу данных или же их включают в CMDB только после того, как они будут введены в работу? Преимущество включения в базу данных продуктов, находящихся на стадии разработки, состоит в том, что в этом случае их спецификации уже нельзя будет менять без получения одобрения, и их передача в рабочую среду будет происходить согласованно. От этого выбора будет зависеть мониторинг статуса CI в рамках

процесса Управления Конфигурациями, к тому же это позволит расширить диапазон контроля жизненного цикла продукта в рамках этого процесса.

Уровень Детализации CMDB

Определение Уровня Детализации для каждого типа Конфигурационных Единиц является важным этапом разработки процесса Управления Конфигурациями. Здесь нет универсальных решений. На этом этапе анализируется информация о Конфигурационных Единицах. Для определения Уровня Детализации составляется схема взаимоотношений между задействованными Конфигурационными Единицами и выбирается требуемая глубина детализации CMDB. Кроме того, определяются имена и атрибуты для Конфигурационных Единиц.

При определении глубины Конфигурационной Базы Данных и взаимоотношений между Конфигурационными Единицами, отражаемыми в CMDB, нужно добиться сбалансированности требований к CMDB — с одной стороны, и загруженности персонала и имеющихся ресурсов — с другой. Количество взаимоотношений растет экспоненциально количеству уровней.

Взаимоотношения между Конфигурационными Единицами

Информация о взаимоотношениях между Конфигурационными Единицами является очень полезной для диагностики ошибок и прогнозирования доступности услуг. Можно определить много разных типов взаимоотношений на логическом и физическом уровнях.

■ Взаимоотношения на физическом уровне:

- *Является частью:* это взаимоотношения типа «parent/child» («родитель/ребенок»), например, дисковод является частью РС, а программный модуль — частью программы.
- *Подключена к:* например, РС подсоединен к сегменту сети.
- *Требуется для:* например, технические средства требуются для работы приложения.

■ Взаимоотношения на логическом уровне:

- *Является копией:* что-то является копией стандартного модуля, Базисной Конфигурации или программы.
- *Связано с:* процедурой, руководством и документацией, Соглашением об Уровне Услуг или группой заказчиков.
- *Используется:* например, Конфигурационная Единица, участвующая в предоставлении услуги, или программный модуль, к которому обращаются несколько программ.

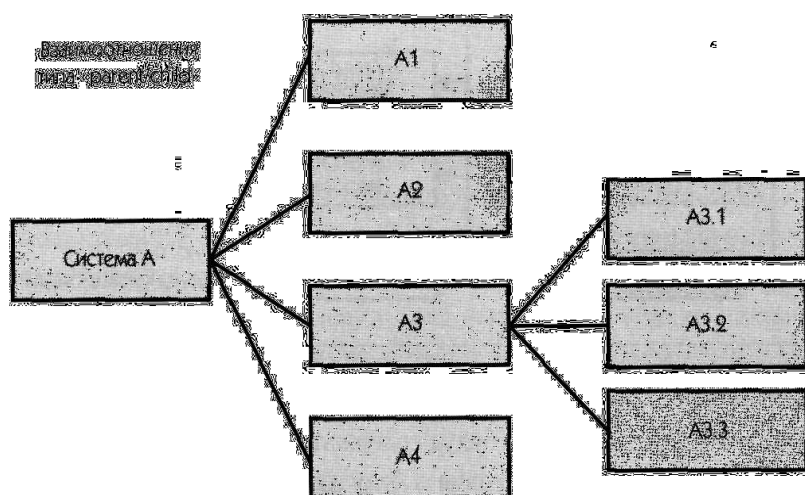


Рис. 6.4. Взаимоотношения между Конфигурационными Единицами типа «parent/child» («родитель/ребенок») (источник: OGC)

Глубина CMDB

При определении Уровней Конфигурационных Единиц создается иерархия компонентов и элементов. Выбираются родительские Конфигурационные Единицы и определяется количество

уровней, необходимых для их детализации. На самом высоком уровне находится сама ИТ-инфраструктура. Самым низким уровнем является наиболее детальный уровень, на котором необходимо осуществлять контроль. Включение Конфигурационных Единиц в Конфигурационную Базу Данных будет целесообразным только в том случае, если информация об этих СИ будет полезна для других процессов ИТIL. Определяя уровни и глубину Конфигурационной Базы Данных, следует помнить, что изменение в любой Конфигурационной Единице, зарегистрированной в CMDB, должно пройти через формальный процесс. Поэтому регистрируя такой компонент как компьютерная мышь в Конфигурационной Базе Данных, создается ситуация, при которой любой Запрос на новую мышь уже не будет проходить как Запрос на Обслуживание¹, а должен будет проводиться через процесс Управления Изменениями в форме Запроса на Изменение (RFC). Это показательный пример для организаций, которые чрезмерно увлекаются детализацией.

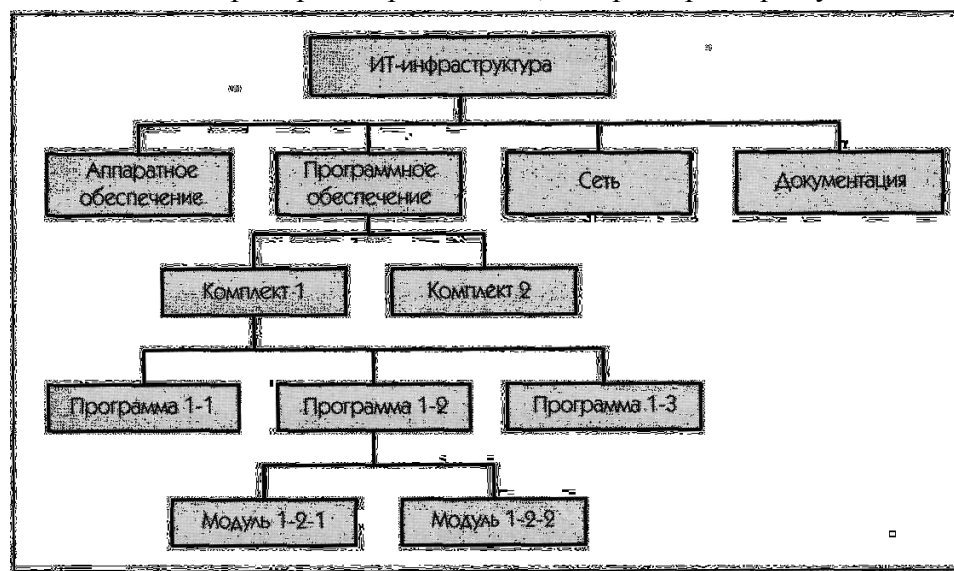


Рис. 6.3. Видеоклип Харви:
Адаптация к CMDB
исходник: OGC

При определении структуры Конфигурационной Базы Данных руководствуются следующими соображениями:

- Чем больше уровней в базе данных, тем больше информации надо обрабатывать. Это ведет к увеличению рабочей нагрузки и созданию более сложной CMDB
- Чем меньше уровней, тем слабее контроль и хранится меньше информации об инфраструктуре.

Если степень детализации CMDB слишком мала, то становится невозможным эффективный мониторинг изменений, происходящих в компонентах нижнего уровня. В этом случае любое изменение в компонентах родительской Конфигурационной Единицы приведет к созданию варианта этой единицы². Например, PC с двумя видами жесткого диска будет проходить как Вариант «А» и Вариант «В». Если в дочернем компоненте много изменений, их нумерация становится сложной и трудной для сопровождения. Однако, если имеются уровни, расположенные ниже, то варианты можно поддерживать на соответствующем уровне. Для дочерних компонентов также можно регистрировать больше атрибутов и связывать с ними известные ошибки. Кроме того, при выполнении диагностики можно ставить такие вопросы, как: «Какой драйвер нужен для этого типа технических средств?», «К какому сегменту подсоединена сетевая плата?» и «Какая программа использует эту библиотеку?».

¹ Service Request.

² Варианты используются, если имеются несколько существующих одновременно форм Конфигурационной Единицы т. е. если существуют параллельные отношения. Версии появляются, например, если одновременно используется и новая, и старая версии Конфигурационной Единицы, т. е. когда существуют последовательные отношения. Использование этих двух концептуальных понятий помогает при планировании изменений. Если в последующем каждый из вариантов будет разрабатываться отдельно, то для каждого из них нужно вводить отдельную систему нумерации версий, что нежелательно, т. к. это делает ИТ-инфраструктуру более сложной и ведет к увеличению работ по сопровождению. В большинстве случаев рекомендуется продолжать разработку исходного экземпляра всех вариантов, а там, где возможно, использовать новую версию для создания необходимых вариантов. - Прим. автора.

Соглашения о присвоении имен¹

У каждой Конфигурационной Единицы должно быть уникальное имя, которое отличает его от других единиц. Самым элементарным вариантом является простая система присвоения номеров с возможным делением на диапазоны для каждой области. Для вновь созданной Конфигурационной Единицы генерируется новый номер. Имена, по возможности, должны иметь смысловое значение для облегчения контактов с пользователями.

Соглашения о присвоении имен также можно использовать для физической маркировки Конфигурационных Единиц, для упрощения их идентификации при инвентаризации (аудите), в процессе сопровождения и регистрации инцидентов. Некоторые из предложенных библиотекой ИТЛ правил присвоения имен:

Метки на аппаратных средствах должны быть легко различимыми и легкими в чтении для пользователей, они должны прочно фиксироваться на поверхности. По договоренности со сторонним поставщиком услуг, в договорах о поддержке могут существовать ссылки на эти метки. Пользователи также должны указывать метки при сообщении об инциденте.

Контролируемые документы, такие как Соглашения об Уровне Услуг (SLA), процедуры и организационные схемы должны маркироваться с указанием номера Конфигурационной Единицы, номера версии и даты выпуска версии.

Копии программного обеспечения должны храниться в Библиотеке эталонного программного обеспечения² (DSL), см. главу «Управление Релизами». Все компоненты программного обеспечения должны иметь номер CI, а инсталлированное ПО еще и номер версии и номер копии.

Атрибуты

Помимо структуры Уровней Конфигурационных Единиц, взаимоотношений между ними и соглашений о присвоении имен, детальная проработка модели CMDb также включает в себя описание атрибутов. Атрибуты используются для хранения информации, имеющей отношение к Конфигурационной Единице. При формировании CMDb можно использовать приведенные ниже атрибуты.

Атрибут	Описание
Номер/метка Конфигурационной Единицы или штриховой код	Уникальный идентификатор Конфигурационной Единицы. Часто это номер, автоматически присваиваемый базой данных. Хотя не все Конфигурационные Единицы имеют физические метки, у всех есть уникальный номер
Номер лицензии или серийный номер	Идентификационный номер поставщика в виде серийного номера или номера лицензии
Номер инвентаризационной системы	Инструментальные средства инвентаризации (аудита) часто используют свои собственные идентификаторы, которые в разных областях инфраструктуры могут быть разными. Данный атрибут обеспечивает связь с этой средой
Номер модели/идентификационный номер Каталога	Уникальный идентификатор, используемый в Каталоге Поставщика. У каждой версии модели свой номер, например, PAT-NL-C366-4000-T
Наименование модели	Полное наименование модели, в которое часто входит идентификатор версии, например, PIIMMX400MHZ
Изготовитель	Изготовитель Конфигурационной Единицы
Категория	Классификация Конфигурационной Единицы (например, технические средства, программное обеспечение, документация и т. д.)

¹ Naming convention.

² Definitive Software Library - DSL

Тип	Описание типа Конфигурационной Единицы, предоставляет детальную информацию о категории, например, Аппаратная Конфигурация, пакет программ или программный модуль
Гарантийный срок	Срок действия гарантии
Номер версии	Номер версии Конфигурационной Единицы
Расположение	Месторасположение Конфигурационной Единицы например, библиотека или носитель, на котором находится программное обеспечение, или территория/комната, где находится Конфигурационная Единица
Владелец	Имя владельца или лица, ответственного за Конфигурационную Единицу
Дата начала ответственности	Дата, когда вышеуказанное лицо стало ответственным за Конфигурационную Единицу
Источник/поставщик	Источник Конфигурационной Единицы, например, собственная разработка, закуплена у поставщика «X» и т. д.
Лицензия	Номер лицензии и ссылка на лицензионное соглашение
Дата поставки	Дата поставки Конфигурационной Единицы в организацию
Дата приемки	Дата приемки Конфигурационной Единицы в операционную среду
Статус (текущий)	Текущее состояние Конфигурационной Единицы, например, «в тестировании», «в работе», «выведено из операционной среды»
Статус (запланированный)	Следующий планируемый статус Конфигурационной Единицы с указанием даты и требуемых действий
Стоимость	Стоимость приобретения Конфигурационной Единицы
Остаточная	Текущая стоимость Конфигурационной Единицы с учетом амортизации; амортизационная стоимость
Комментарии	Текстовое поле для комментариев, например, для описания отличий одного варианта от другого

Таблица 6.1. Примеры атрибутов

В зависимости от возможностей используемых инструментальных средств (программного обеспечения) автоматизации Сервис-менеджмента в CMDB включается информация о взаимоотношениях с инцидентами и другие аналогичные им взаимоотношения в виде атрибутов или в какой-либо другой форме.

Атрибут	Описание
Номера запросов на изменения (RFC)	Номер (номера) Запросов на изменение (RFC), открытых в настоящий момент или ранее для данной Конфигурационной Единицы
Номера изменений	Номер (номера) изменений, открытых в настоящий момент или ранее для данной Конфигурационной Единицы
Номера проблем	Номер (номера) проблем, открытых в настоящий момент или ранее для данной Конфигурационной Единицы
Номера инцидентов	Номер (номера) инцидентов, связанных с данной Конфигурационной Единицей

Таблица 6.2. Примеры других записей, связанных с Конфигурационными Единицами

Обычно номера соответствующих Конфигурационных Единиц входят в состав регистрационных записей инцидентов, проблем и изменений. Независимо от выбранного подхода должны поддерживаться взаимоотношения между Конфигурационными Единицами и следующими записями (табл. 2).

Атрибут	Описание
Взаимоотношения с родительскими Конфигурационными Единицами	Ключ или номер родительской Конфигурационной Единицы
Взаимоотношения между дочерними Конфигурационными Единицами	Ключ или номер дочерней Конфигурационной Единицы
Другие взаимоотношения	Взаимоотношения между Конфигурационной Единицей и другими единицами, отличными от родительских и дочерних, например, эта Конфигурационная Единица имеет статус «используется» или «подключена к ...»

Таблица 6.3. Атрибуты взаимоотношений

Как уже обсуждалось, поддержка информации о взаимоотношениях между Конфигурационными Единицами является важным аспектом процесса Управления Конфигурациями. В зависимости от типа базы данных эти взаимоотношения могут быть представлены в виде атрибутов CI или в отдельной таблице.

В некоторых базах данных есть дополнительная возможность для записи изменений содержимого поля, что обеспечивает ведение журнала истории. Это помогает, например, получать информацию о простоях, ремонте, техническом обслуживании по истории состояния поля «Текущий статус», кроме того, это полезно для отслеживания истории владения.

Кроме рассмотренных выше атрибутов, необходимыми являются перечни атрибутов с технической информацией о каждом типе Конфигурационной Единицы. У каждого типа свои характеристики. Например, для PC это емкость жесткого диска, изготовитель BIOS и версия BIOS, размер оперативной памяти, IP-адрес и т. д. Многие инструменты системного администрирования фиксируют такую информацию, в этом случае достаточно установить связь с типом Конфигурационной Единицы, чтобы избежать дублирования информации. Однако следует помнить, что такие системы предоставляют текущую информацию, не указывая, является ли она результатом реализации утвержденных изменений или же это результат неавторизованных действий.

Для облегчения ввода и обновления атрибутов можно использовать открывающиеся меню¹. Можно устанавливать связи и с другими надежными источниками для получения информации о месторасположении Конфигурационной Единицы, пользователях, подразделениях, номерах телефонов, владельцах и параметрах бюджета. Вариантов много, но всегда следует учитывать нагрузку, связанную с поддержкой актуальности этих файлов.

Базисная Конфигурация

Базисная Конфигурация — это мгновенный снимок группы Конфигурационных Единиц, сделанный в определенный момент времени. Базисную Конфигурацию можно использовать в качестве:

- авторизованного/поддерживаемого продукта, который можно включить в ИТ-инфраструктуру; (такие Базисные Конфигурации включаются в Каталог Продуктов);
- стандартных Конфигурационных Единиц для учета информации о стоимости;
- базы² при разработке и тестировании новых Конфигураций;
- для выполнения возврата к исходному состоянию, если возникают проблемы с новой Конфигурацией после проведения изменений;
- стандарта для поставки Конфигураций пользователям, например, «стандартное рабочее место»;
- базы при установке нового программного обеспечения.

¹ Т.е. меню со списком выбора вариантов. - Прим. ред.

² Starting point

Стандартная рабочая станция является типичным примером Базисной Конфигурации. Ограничивая количество разных стандартных рабочих станций, можно облегчить оценку результатов и определение ресурсов, необходимых для реализации новых функций и улучшения их тестирования. Базисные Конфигурации также могут помочь в проведении политики комбинирования и планирования изменений, например, для пакетных релизов. Они способствуют сокращению затрат на Управление и облегчают планирование проектов.

Другим полезным применением Базисной Конфигурации является Каталог Продуктов. В нем даются Сертифицированные Конфигурации, которые можно использовать в ИТ-инфраструктуре и которые доступны для заказа пользователями. В этом случае новая Конфигурационная Единица является копией единицы из Каталога с ее номером и меткой.

До того как новая модель или продукт будут добавлены в инфраструктуру, они должны появиться в Каталоге. Для этого нужно принять решения по трем вопросам:

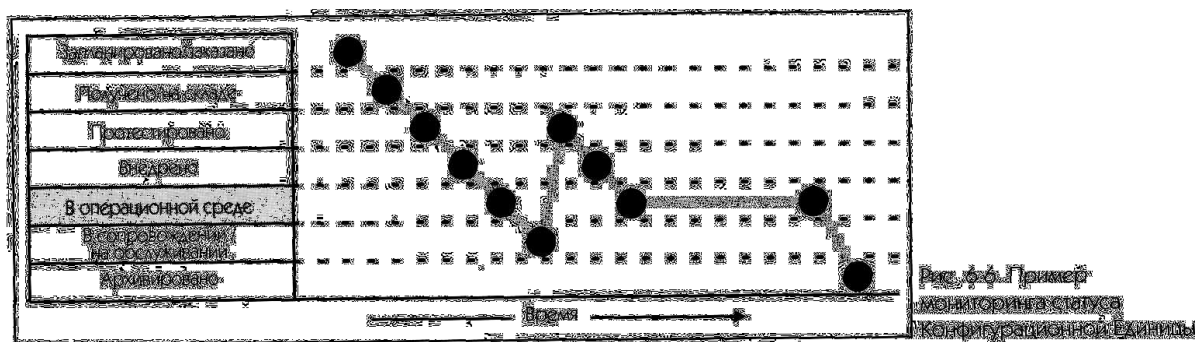
- **Бизнес:** отвечает ли модель/продукт бизнес-интересам пользователя?
- **Финансы:** приемлемы ли затраты на поддержку?
- **Влияние:** приемлем ли уровень воздействия модели/продукта на услугу?

Регистрация

Первоначально База данных CMDB наполняется информацией из финансовых систем, записями о существующей ИТ-инфраструктуре, техническими данными от поставщиков. Регистрируется только информация из известных (проверенных) источников. Организация должна быть готова к поддержанию этой информации в актуальном состоянии.

6.4.3. Мониторинг статуса

Цикл жизни компонента можно разделить на несколько этапов, каждому из которых присваивается свой статус. Этапы зависят от тех характеристик ИТ-инфраструктуры, которые организация хочет регистрировать. Регистрация даты каждого изменения статуса дает важную информацию о жизненном цикле продукта: о времени заказа, времени инсталляции, о сопровождении и поддержке продукта.



Статус компонента также помогает определить, какие действия можно выполнять с ним. Например, если составлен отчет об элементах со статусом «неэксплуатирующиеся запасные части», то эти технические средства нельзя перераспределять куда-либо еще без предварительного согласования, например, в рамках развертывания плана восстановления после чрезвычайных ситуаций. Изменение статуса Конфигурационной Единицы может быть вызвано авторизованными или неавторизованными изменениями или инцидентами.

Может быть использована следующая классификация статусов.

- **Новые Конфигурационные Единицы:**
 - В разработке/заказе;
 - Протестирована;
 - Принята (по результатам тестирования).
- **Существующие Конфигурационные Единицы:**
 - Получена (принята в операционную среду);

- Открыт Запрос на Изменение (RFC) Конфигурационной Единицы, запрошена новая версия;
 - Изменение утверждено и включено в план изменений, новая Конфигурационная Единица и документация (также являющаяся Конфигурационной Единицей) будут предоставлены;
 - На обслуживании;
 - Не функционирует.
- **Архивированные Конфигурационные Единицы:**
- Выведена из операционной среды;
 - Исключена (deleted);
 - Удалена (removed);
 - Похищена;
 - Продана или истек срок аренды/лизинга;
 - В архиве в ожидании безвозмездного дарения, продажи или уничтожения;
 - Уничтожена.
- **Все Конфигурационные Единицы:**
- В наличии;
 - Получена по заказу или доступна новая версия; • - Тестируется;
 - Одобрена для инсталляции;
 - Активная Конфигурационная Единица находится в использовании;
 - Запасные части.

6.4.4. Контроль

Для поддержания Конфигурационной Базы (CMDB) в актуальном состоянии необходимо эффективное Управление Информацией. При любом изменении зарегистрированных характеристик Конфигурационных Единиц или взаимоотношений между ними, вызванном выполнением любого действия, это изменение должно быть отражено в базе данных.

Примечание. Изменять характеристики Конфигурационных Единиц можно только путем проведения изменений авторизованных процессом Управления Изменениями; Управление Инцидентами может изменять только статус существующих Конфигурационных Единиц.

Управление Конфигурациями контролирует все ИТ-компоненты, существующие в организации, и отвечает за их регистрацию в системе. Аппаратные средства можно регистрировать при их заказе или получении, а программное обеспечение — при его включении в Библиотеку эталонного программного обеспечения (Definitive Software Library — DSL).

Одна из задач контроля — гарантировать регистрацию только авторизованных и включенных в Каталог Продуктов Конфигурационных Единиц. Для этого должно быть организовано активное взаимодействие процесса Управления Конфигурациями с поставщиками и процессами Управления Инцидентами, Проблемами и Изменениями.

Если по согласованию с Управлением Изменениями произведены некоторые изменения в ИТ-инфраструктуре, процесс Управления Конфигурациями обязан отразить эти изменения в Конфигурационной Базе Данных. Хотя публикации ITIL не дают четких указаний по этому вопросу, на практике ответственность за регистрацию Запросов на Изменение (RFC) происходит под контролем процесса Управления Изменениями¹. Формализованные записи об изменениях являются основным источником информации об изменениях в инфраструктуре, которая используется для обновления Конфигурационной Базы Данных. По существу процесс Управления Конфигурациями

¹ В то же время Управление Конфигурациями сохраняет наивысшую ответственность за актуальность Конфигурационной Базы Лунных, то есть возможно делегирование полномочий (но не ответственности) по регистрации результатов изменений из процесса Управления Конфигурациями в процесс Управления Изменениями. — Прим. ред.

предъявляет требования к уровню зрелости процессов в организации, особенно к Управлению Изменениями, операционной средой и проведения закупок.

Для того, чтобы авторизованная Конфигурационная База Данных отражала реальную ситуацию, необходимо проводить мониторинг следующих действий:

- добавление Конфигурационной Единицы;
- изменение статуса Конфигурационной Единицы, например, «работает» или «не работает» (полезно для процесса Управления Доступностью);
- изменение владельца Конфигурационной Единицы;
- изменение взаимоотношений Конфигурационной Единицы с другими Конфигурационными Единицами;
- удаление Конфигурационной Единицы;
- возникновение новых взаимоотношений Конфигурационной Единицы с каким-либо сервисом, другой Конфигурационной Единицей, документацией и т. д.;
- возобновление или изменение лицензии;
- обновление детальной информации о Конфигурационной Единице после аудита.

6.4.5. Верификация и аудит

Аудит проводится для проверки, насколько точно отражена текущая ситуация в CMDB. Например, инструментальные средства аудита могут автоматически выполнять анализ рабочих станций и формировать отчеты о текущей ситуации и статусе ИТ-инфраструктуры. Эта информация будет использоваться для проверки и обновления Конфигурационной Базы Данных. Аудит возможен в следующих ситуациях:

- после внедрения новой Конфигурационной Базы Данных;
- к примеру, спустя полгода с момента внедрения;
- перед серьезными изменениями и после них;
- после чрезвычайных обстоятельств;
- в любое другое удобное время.

При проведении аудита рассматриваются следующие вопросы:

- Регистрируются ли в CMDB данные всех Запросов на Изменения на всех этапах их реализации, и контролирует ли процесс Управления Конфигурациями эту регистрацию?
- Находится ли Конфигурационная База Данных в актуальном состоянии, если нет, то почему? Какое воздействие это оказывает на процесс Управления Изменениями (анализ текущего воздействия запланированных изменений)?
- Производится ли присвоение имен новым Конфигурационным Единицам в соответствии с соглашением о присвоении имен?
- Правильно ли используются варианты? Правильно ли регистрируются Базисные Конфигурации и становятся ли они сразу же доступными к использованию?
- Соответствует ли содержимое Библиотеки эталонного программного обеспечения (DSL) и Склада эталонного аппаратного обеспечения (DHS) информации в Конфигурационной Базе Данных? Если нет, то почему?

Аудиторские проверки также можно проводить, выбирая объекты случайным образом или проводить там, где Руководитель Процесса Управления Конфигурациями считает, что информация может быть некорректной. Если существует связь с автоматическими инструментальными средствами аудита, тогда можно делать аудит соответствующих областей или формировать по ним дельта-отчеты практически ежедневно.

Если обнаруживаются расхождения, то инструментальные средства аудита не должны автоматически обновлять Конфигурационную Базу Данных. Все расхождения свидетельствуют о том, что изменения были произведены в обход процесса Управления Изменениями, и теперь эти прецеденты должны быть изучены.

6.5. Контроль процесса

6.5.1. Отчеты и Ключевые показатели эффективности

В отчет по процессу Управления Конфигурациями возможно включение следующей информации:

- информация о качестве процесса;
- расхождения между регистрационными записями и реальной ситуацией, обнаруженные во время аудита (дельта);
- количество случаев, когда используется неавторизованная Конфигурация;
- количество случаев, когда зарегистрированная Конфигурация не находилась на своем месте;
- отклонения на Уровне Атрибутов, обнаруженные аудиторскими проверками;
- длительность обработки Запросов на Регистрацию информации;
- перечень Конфигурационных Единиц, в отношении которых количество зарегистрированных инцидентов или изменений превышало заданную величину;
- статистическая информация о структуре и составе ИТ-инфраструктуры;
- данные о росте и другая информация о развитии ИТ-инфраструктуры;
- сводные данные, отчеты и предложения по улучшению, например, рекомендации по изменению охвата(границ) процесса и Уровня Конфигурационных Единиц, отслеживаемых процессом Управления Конфигурациями, связанные с изменениями в бизнесе, технических средствах, рыночных ценах и т. д.;
- расходы на персонал при внедрении процесса.

6.5.2. Критические факторы успеха

Условием успешной работы по Управлению Конфигурациями является получение необходимой информации для поддержания базы данных в актуальном состоянии. Это означает, что обязательно нужно поддерживать взаимосвязи с процессом Управлением Изменениями, а для регистрируемых характеристик всегда должен быть найден тот, кому они требуются.

Внедрение процесса важно правильно разбить на этапы. Попытки ввести требование регистрации компонентов инфраструктуры без соответствующей подготовки обычно заканчиваются неудачей, т. к. дисциплина, необходимая для Управления Конфигурациями, не может появиться мгновенно. Записи, которые велись до ввода процесса, должны быть выведены из обращения во избежание дублирования. При запуске процесса в работу важно продемонстрировать несколько явных преимуществ, которые дает Управление Конфигурациями (быстрые успехи¹). Кроме того, важно, чтобы обязанности по регистрации были закреплены за теми сотрудниками, у кого есть не только необходимые навыки, но и должное отношение к работе.

6.5.3. Функции и роли

Работа процессов происходит в горизонтальной плоскости, относительно вертикальной иерархической структуры организации. Это возможно только при четком распределении ответственностей и полномочий по их реализации. Для повышения гибкости может быть использован ролевой подход. В небольших организациях или в силу экономических причин возможно комбинирование ролей, например, Руководителя Процесса Управления Изменениями и Управления Конфигурациями. В задачи Руководителя Процесса Управления Конфигурациями может входить следующее:

- предложения по изменению сферы действия и Уровня Детализации Процесса Управления Конфигурациями;
- информированность всей организации о существующем Процессе Управления Конфигурациями;
- обеспечение процесса персоналом и его обучение;
- разработка системы идентификации и соглашений о присвоении имен;

¹ Quick wins.

- разработка интерфейсов с другими процессами;
- оценка существующих систем и внедрение новых систем автоматизации процесса;
- планирование и внедрение системы наполнения информации в Конфигурационной Базе Данных;
- формирование отчетов;
- организация аудиторских проверок.

6.6. Затраты и проблемы

6.6.1. Затраты

Расходы на запуск и реализацию процесса Управления Конфигурациями во многом зависят от области действия и Уровня Детализации Процесса. В число расходов входят затраты на аппаратное и программное обеспечение и персонал. Расходы на аппаратное и программное обеспечение состоят из затрат на:

- дополнительные технические средства и их конфигурирование;
- дополнительное программное обеспечение и его конфигурирование;
- лицензии, пропорционально количеству пользователей;
- разработку приложений и базы данных, наполнение их данными, настройку на требования заказчика и внедрение;
- поддержку и сопровождение базы данных;
- дополнительный персонал, необходимый для работы процесса.

6.6.2. Проблемы

ИТ-организация должна четко определить свои намерения относительно того, какие характеристики ИТ-инфраструктуры должны регистрироваться и обеспечить необходимые руководящие ресурсы для исполнения намеченного. В организации должна существовать твердая приверженность в использовании Конфигурационной Базы Данных (CMDB). Необходимо произвести перенос всех ранее использованных данных из других баз в CMDB.

На успешную реализацию процесса могут повлиять следующие проблемы:

▪ **Неправильно определен охват (границы) Конфигурационной Базы Данных или Уровень Детализации Конфигурационных Единиц** — если сфера действия Конфигурационной Базы Данных слишком мала, то важные части инфраструктуры будет невозможно проверить, исправить, защитить или восстановить. Если же наоборот охват слишком большой, то громоздкость базы данных будет препятствием, замедляющим все процессы Сервис-менеджмента. При большом количестве уровней, атрибутов и взаимоотношений будет трудно поддерживать базу данных в актуальном состоянии. Слишком низкий Уровень Детализации приведет к регистрации неполной информации о Конфигурационных Единицах и связанных с ними инцидентах, проблемах, известных ошибках и запросах на Изменение.

▪ **Неадекватная система ручной обработки** — некоторые организации стараются как можно дольше хранить данные на бумажных носителях и покупают автоматизированные средства только тогда, когда работать становится невозможно. Это может приводить к задержкам в работе, путанице, потере персонала и ресурсов и т. д. Рекомендуется закупать автоматизированные средства обработки как можно раньше, ориентируясь на функциональные требования процесса.

▪ **Влияние срочных изменений** — всегда будут возникать ситуации, когда нужно срочно произвести изменение. Часто это происходит во внерабочее время. Если изменяемые Конфигурационные Единицы находятся под контролем Конфигурационной Базы Данных, то рекомендуется немедленно произвести запись результатов изменения в CMDB, но может возникнуть ситуация, когда отсутствует сотрудник, ответственный за эту задачу. В этом случае регистрацию изменений и обновление CMDB необходимо будет сделать при первой возможности.

▪ **Чрезмерно плотный график работы** — если график изменений (Запросов на Изменения) не оставляет времени на выполнение действий в рамках процесса Управления Конфигурациями, то в

работе могут появляться задержки и данный процесс будет восприниматься как препятствие. Следует составлять реалистичные графики, основываясь на прошлом опыте.

- **Понимание руководством важности процесса** — поскольку Управление Конфигурациями является относительно новым процессом, не всегда достаточно видимым для сотрудников, персонал может сопротивляться его принятию. Должна быть достаточная приверженность к необходимости процесса со стороны руководства. Поэтому руководитель процесса должен информировать об Управлении Конфигурациями сотрудников компании и пропагандировать этот процесс в компании. Опыт показывает, что затраты на реализацию процесса будут значительно ниже, если процесс Управления Конфигурациями представлен в компании как отдельная дисциплина с закрепленным за ней персоналом и руководителем, отвечающим за процесс.

- **Попытки обхода процесса** — в состоянии спешки персонал может пытаться обойти правила работы процесса Управления Конфигурациями. Если такая ситуация возникает регулярно, то после разъяснения негативных последствий таких действий возможно принятие дисциплинарных мер.

Глава 7

Управление Изменениями

7.1. Введение

Быстрое развитие ИТ-технологий и рынка привели к тому, что сейчас изменения стали обычным делом. Однако опыт показывает, что инциденты, влияющие на бизнес-приложения, часто бывают вызваны изменениями. Причины таких инцидентов могут быть различными: халатность сотрудников, недостаток ресурсов, недостаточная подготовка, слабый анализ воздействия изменения, несовершенство испытаний или «болезни роста». Если инциденты, связанные с изменениями, не будут контролироваться, из-под контроля может выйти все предоставление ИТ-услуг и сам бизнес. Число инцидентов может увеличиваться, каждый из них будет требовать принятия срочных мер, что в свою очередь может привести к возникновению новых инцидентов. Ежедневное планирование часто не в состоянии учитывать увеличивающуюся рабочую нагрузку. Это может повлиять на повседневную работу и на сопровождение ИТ-услуг.

Целью Процесса Управления Изменениями является руководство проведением изменений и ограничение числа инцидентов, вызванных изменениями. Девиз Процесса Управления Изменениями:

Не всякое изменение является улучшением, но всякое ухудшение является изменением.

На рис. 7.1 показан цикл изменений, вызванный предложениями на новые разработки и улучшения (Процессы Предоставления услуг и Управления Проблемами), Запросами (адресованными в Процесс Управления Изменениями) и требуемыми решениями (Процесс Управления Проблемами):

- **Инновации и усовершенствования** — внедрение новых услуг и новых технических средств в ИТ инфраструктуру становится причиной появления новых регулярно возникающих ошибок¹ в ИТ-инфраструктуре.

- **Изменения** — все, от небольших инсталляций до перестановки мейнфреймов, при неаккуратном проведении изменений могут стать причиной появления новых регулярно возникающих ошибок в ИТ-инфраструктуре.

- **Корректирующие меры** — нацелены на исправление недавно появившихся регулярно возникающих ошибок.

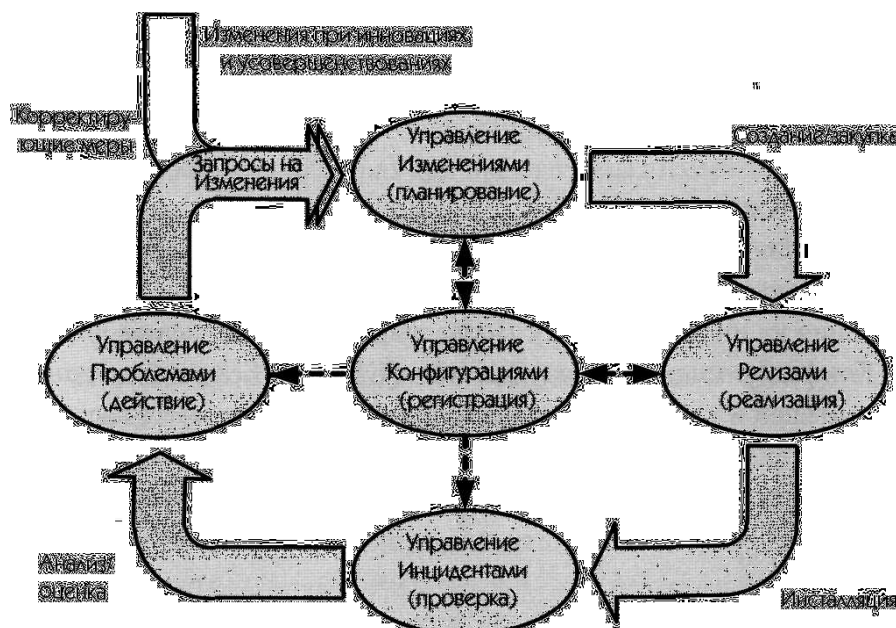


Рис. 7.1. Входы Процесса Управления Изменениями

¹ Long-term errors

Управление Изменениями действует как терморегулятор между **гибкостью** (одобрение изменений, которые могут привести к долгосрочным ошибкам) и **стабильностью** (одобрение изменений для исправления долгосрочных ошибок). Корректирующие меры уменьшают число инцидентов, за счет чего снижается рабочая нагрузка. Возвращаясь к аналогии с терморегулятором, можно сказать, что температура воды соответствует Уровню Изменений и Инноваций, с которой организация может справиться. Новые дома оборудуются душами с терморегуляторами, автоматически компенсирующими любые изменения давления воды. Если кто-либо и откроет кран холодной воды где-нибудь в доме, принимающий душ не ошпарится.

7.1.1. Основные термины

Две точки принятия решения об изменениях

Существуют две точки принятия решения о проведении изменений:

▪ **Руководитель Процесса Управления Изменениями** — лицо, ответственное за предварительный просмотр (фильтрацию) и классификацию Запросов на Изменения¹ (RFC). В больших организациях в помощь Руководителю Процесса могут существовать Координаторы изменений, осуществляющие взаимодействие между ним и различными подразделениями организации. Одной из задач Процесса Управления Изменениями является получение требуемой авторизации изменения. В определенной степени сам процесс уже имеет полномочия, но для проведения некоторых изменений может потребоваться согласование с руководством ИТ (например, с Руководящим комитетом² или Исполнительным комитетом³). Руководитель Процесса Управления Изменениями также несет ответственность за планирование и координацию проведения изменений.

▪ **Консультативный комитет по изменениям⁴ (CAB)** — консультативный орган, регулярно собирающийся для оценки и планирования изменений. Чаще всего одно или несколько значительных изменений выносятся на обсуждение Комитета. Отдельно создается комитет по срочным изменениям⁵ (EC), который назначается руководством для принятия чрезвычайных решений. Состав Консультативного комитета является гибким и включает представителей всех основных ИТ-подразделений:

- Руководителя по Управлению Изменениями (председатель);
- Руководителя по Управлению (Уровнями) Услуг;
- Представителей Службы Service Desk и Процесса Управления Проблемами;
- Руководителей линейных подразделений компании;
- Бизнес-руководителей (или их представители) со стороны заказчика;
- Представителей пользователей;
- Представителей разработчиков приложений; Администраторов программного обеспечения и системных администраторов;
- Представителей поставщиков.

Охват (сфера действия или границы)⁶ процесса

Сфера действия Процесса Управления Изменениями определяется вместе со сферой действия Процесса Управления Конфигурациями, так как Управление Конфигурациями предоставляет информацию для оценки воздействия изменения на инфраструктуру. После проведения изменения Управление Конфигурациями обновляет Конфигурационную Базу Данных (CMDB). Если в базе данных CMDB ведется учет компьютерных мышей и клавиатур, то замена клавиатуры рассматривается как изменение. Определение сферы действия процесса является динамической

¹ Request For Change - RFC

² Steering Committee

³ Executive Committee

⁴ Change Advisory Board — CAB.

⁵ Emergency Committee - EC.

⁶ Scope

деятельностью, так как сфера действия может меняться, и потребность в информации из базы данных CMDB также меняется. Следовательно, сфера действия должна регулярно пересматриваться, и модель данных CMDB должна обновляться соответственно.

Для того, чтобы обеспечить эффективное взаимодействие Процессов Управления Изменениями и Управления Конфигурациями, необходимо регистрировать изменения и обновлять соответствующие записи в CMDB. Можно допустить, что ряд повседневных заданий, точно определенных и подчиняющихся установленным процедурам (т. е. стандартных заданий), не требуют контроля ее стороны Процесса Управления Изменениями. Примерами таких заданий могут быть установка кассет для резервного копирования, создание идентификаторов (ID) пользователей и т. д. Эти действия не обрабатываются как изменения, а самое большее классифицируются как Запросы на Обслуживание в рамках Процесса Управления Инцидентами. Внимательное изучение стандартных действий может быть полезно для предотвращения излишней бюрократизации Процесса Управления Изменениями.

Одним из способов выполнения таких действий является определение так называемых «предварительно авторизованных»¹ изменений (или «категории 0»), которые записываются в базу данных изменений (предпочтительно самими запрашивающими), но не требуют использования процедур по Управлению Изменениями. Например, если при приеме на работу нового сотрудника обычно выполняются четырнадцать действий (создание новой учетной записи², настройка рабочей станции электронной почты и т. д.), то эти действия не требуют столь внимательного изучения, как значительные изменения инфраструктуры. Такой вид стандартных изменений обрабатывается по типовому шаблону как предварительно авторизованный «Запрос на Обслуживание».

7.2. Цель процесса

Целью Процесса Управления Изменениями является гарантия использования стандартных методов и процедур для быстрой обработки изменений с минимальным возможным отрицательным воздействием изменения на качество услуг. Все изменения должны быть отслеживаемыми, чтобы можно было ответить на вопрос: «Что изменилось?»

7.2.1. Преимущества использования процесса

Для эффективного предоставления ИТ-услуг организация должна уметь обрабатывать большое количество изменений с надлежащим Уровнем Ответственности при принятии решений.

Преимуществами Процесса Управления Изменениями являются:

- уменьшение отрицательного воздействия изменений на качество ИТ-услуг;
- более точные оценки затрат для предлагаемых изменений;
- уменьшение количества изменений, потребовавших возврата к исходному состоянию, и каждый такой возврат происходит более гладко;
- предоставление руководству более полной информации об изменениях, что позволяет выявлять проблемные области;
- повышение производительности работы пользователей за счет более высокой стабильности и качества ИТ-услуг;
- повышение производительности работы ИТ-персонала, не отрывающегося от плановой работы для проведения срочных изменений и процедур возврата;
- рост способности компании проводить частые изменения без нарушения стабильности ИТ-среды

7.3. Процесс

Процесс Управления Изменениями принимает или отклоняет каждый Запрос на Изменение (RFC). Руководитель Процесса Управления Изменениями содействует работе процесса, но

¹ Pre-authorized.

² Account.

реальные решения о наиболее значительных изменениях принимаются консультативным комитетом по изменениям (CAB). Членами комитета CAB являются представители разных отделов компании, а также заказчиков и поставщиков. Ответственность за предоставление информации о потенциальном воздействии предлагаемых изменений несет Процесс Управления Конфигурациями.



Рис. 7.2. Позиционирование Процесса Управления Изменениями

Входы Процесса Управления Изменениями включают в себя:

- Запросы на Изменения (RFC);
- информация из базы данных CMDB (в частности, анализ степени воздействия изменений);
- информация из других процессов (из Базы данных мощностей CDB, информация о бюджете и т. д.);
- планирование изменений (Согласованный план изменений¹ FSC).

Выходы процесса включают:

- обновленный план изменений (Согласованный план изменений FSC);
- моменты инициирования действий (триггеры) в рамках Процессов Управления Конфигурациями и Управления Релизами;
- повестка дня Консультативного комитета CAB, протоколы и принятые решения;
- отчеты по Процессу Управления Изменениями.

Управление Изменениями имеет описанную ниже взаимосвязь с другими процессами.

7.3.1. Управление Инцидентами

Процесс Управления Инцидентами имеет двухстороннюю связь с Процессом Управления Изменениями. С одной стороны, Управление Изменениями обрабатывает направляемые Управлением Инцидентами Запросы на Изменения для разрешения инцидента или запрашиваемые Управлением Проблемами изменения, устраняющие причину инцидента. С другой стороны, несмотря на многочисленные предосторожности, внедрение изменений все же может привести к возникновению инцидентов. Это может быть связано с ошибками проведения изменения или с недостаточной подготовкой пользователей к изменениям. Соответствующий персонал Управления Инцидентами должен быть информирован о проведении изменений, чтобы иметь возможность быстро определить и устранить возникающие инциденты.

¹ Forward Schedule of Change - FSC.

7.3.2. Управление Конфигурациями

Управление Изменениями и Управление Конфигурациями являются настолько тесно связанными процессами, что они могут быть эффективно интегрированы между собой — шаг, рекомендованный в библиотеке ИТЛ.

Изменения регистрируются под контролем Процесса Управления Конфигурациями, анализ воздействия изменений также проводится с участием Процесса Управления Конфигурациями. Управление Конфигурациями определяет зависимость между Конфигурационной Единицей СИ (вовлеченной в проводимое изменение) и другими СИ, чтобы определить, на какие другие элементы будет воздействовать это изменение.

7.3.3. Управление Проблемами

Взаимосвязь между Процессами Управления Изменениями и Управления Проблемами во многом похожа на такую же связь между Процессами Управления Изменениями и Управления Инцидентами. С одной стороны, изменения часто бывают необходимы для разрешения проблем. С другой стороны, если проведение изменений недостаточно контролируется, они могут привести к новым проблемам.

7.3.4. Управление Релизами

Изменения часто приводят к необходимости разработки и распространения новых приложений или установке технической инфраструктуры. Это осуществляется с помощью Процесса Управления Релизами. Контроль над распространением новых версий осуществляется Процессом Управления Изменениями.

7.3.5. Управление Уровнем Сервиса

Процесс Управления Уровнем Сервиса вовлечен в определение степени воздействия изменений на предоставление услуг и бизнес-процессы. В зависимости от ситуации в Консультативном комитете (СAB) могут участвовать представители Процесса Управления Уровнем Сервиса. Если изменение оказывает значительное воздействие или связано с высоким риском, его внедрение и сроки должны всегда обсуждаться с заказчиком. Управление Изменениями направляет в Управление Уровнем Услуг отчет «Проектируемая доступность услуг»¹ (PSA). В этом отчете Управление Изменениями излагает изменения в имеющихся Соглашениях об Уровне Услуг (SLA) и воздействие Согласованного плана изменений (FSC) на доступность услуг.

7.3.6. Управление Доступностью

Процесс Управления Доступностью инициирует изменения, направленные на повышение доступности услуг и проверяет, привели ли предпринимаемые меры к ожидаемому результату. Управление Доступностью часто привлекается при оценке потенциального воздействия изменений, так как это воздействие может повлиять на доступность услуги.

7.3.7. Управление Мощностями

Руководитель Процесса Управления Мощностями в первую очередь занимается вопросом анализа совокупного эффекта по результатам изменений в течение продолжительного периода времени, например, увеличением времени реакции приложений или потребностью в большей емкости для хранения информации. На основе составленного Плана мощностей Управление Мощностями регулярно предлагает усовершенствования и инициирует изменения в форме Запросов на Изменения (RFC).

7.3.8. Управление Непрерывностью ИТ-услуг

Превентивные мероприятия и планы восстановления, гарантирующие непрерывность услуг, должны постоянно контролироваться, так как изменения инфраструктуры могут сделать эти планы

¹ Projected Service Availability - PSA.

неосуществимыми или избыточными. Процесс Управления Изменениями действует в тесной взаимосвязи с Процессом Управления Непрерывностью ИТ-услуг, чтобы в нем учитывались все изменения, которые могут повлиять на планы восстановления, и предусматривались меры, необходимые для проведения восстановления.

7.3.9. Виды деятельности в рамках Процесса Управления Изменениями

Процесс Управления Изменениями включает в себя следующие виды деятельности для обработки изменений:

- **Прием в обработку** — предварительный просмотр (фильтрация) Запросов на Изменения и прием их к дальнейшему рассмотрению.

- **Планирование** — объединение изменений, планирование их проведения и планирование необходимых ресурсов.

- **Оценка** — оценка успешности каждого изменения и составление заключения для будущей деятельности (накопление знаний).

Рис. 7.3. Виды деятельности в рамках Процесса Управления Изменениями

7.4. Виды деятельности

7.4.1. Регистрация

Прежде всего, все Запросы на Изменения (RFC) должны быть зарегистрированы. При подаче Запроса на Изменение для решения проблемы также регистрируется номер известной ошибки.

Что представляет собой Запрос на Изменения (RFC)?

Не каждый Запрос на Модификацию обрабатывается как изменение: некоторые повседневные задания, точно определенные и подчиняющиеся установленным процедурам (стандартизованные), но включающие в себя модификации, могут обрабатываться как Запросы на Обслуживание (на пример, изменения «категории 0», см. 7.1.1). В результате возникает следующая классификация изменений:

- **Запросы на Обслуживание (здесь: стандартные изменения)** — полностью определенные и утвержденные изменения, регистрируемые, но не оценивающиеся Процессом Управления Изменениями. Эти изменения проводятся в рабочем порядке. (*Примечание.* Не все Запросы на Обслуживание являются изменениями).
- **Запросы на Изменения** — все другие Запросы на Модификацию инфраструктуры.

Откуда исходят Запросы на Изменения (RFC)?

Запросы на Изменения могут касаться всех аспектов инфраструктуры в пределах сфер] действия процессов ITIL. Любой сотрудник, работающий с инфраструктурой, может подать Запрос на Изменения (RFC). Можно определить несколько источников Запросов на Изменения (RFC), например:

- **Управление Проблемами** — предлагает решения для исключения долговременных ошибок с целью стабилизации предоставления услуг.
- **Заказчики** — могут запросить больший, меньший Уровень Сервиса или другие услуги. Эти запросы могут подаваться прямо как Запрос на Изменения или направляться через Управление Уровнем Сервиса (SLM) или через Управление Отношениями с заказчиками ИТ (IT CRM).
- **Политика компании** — тактические и стратегические процессы из области Предоставления услуг (Service Delivery Set) и Указания руководства (Managers Set) могут привести к направлению Запросов на Изменение Услуг. Например, Управление Уровнем Услуг, Управление Доступностью, Управление Мощностями составляют ежегодные планы улучшения услуг, которые позднее могут быть поданы как Запросы на Изменения (RFC).
- **Законодательство** — если возникают ограничения, регламентирующие бизнес-деятельность, или вводятся новые требования по ИТ-безопасности, непрерывности бизнес-процессов и Управлению Лицензиями.
- **Поставщики** — поставщики выпускают новые версии и модификации¹ своих продуктов и сообщают об исправленных ими ошибках. Они могут сообщить, что больше не поддерживают определенные версии или что не могут гарантировать производительность версии (например, из-за «Ошибки тысячелетия» — Millennium bug). Это может дать толчок Процессам Управления Проблемами или Управления Доступностью к подаче Запроса на Изменения (RFC).
- **Проекты** — проект часто вызывает ряд изменений. Руководство проекта должно эффективно согласовывать свои действия с Управлением Изменениями с помощью соответствующих таких как Управление Уровнем Услуг, Управление Мощностями и т. п.
- **Любой другой сотрудник ИТ** — в принципе, любой сотрудник может подать предложения улучшению услуг. В особенности, ИТ-персонал может способствовать усовершенствованию процедур по поддержке и предоставлению услуг и обновлению руководств.

¹ Upgrades.

Регистрация Запросов на Изменения

Вот примеры информации, которая может включаться в Запросы на Изменения (RFC):

- идентификационный номер Запроса;
- номер проблемы/известной ошибки (если имеется), связанной с Запросом;
- описание и определение соответствующих Конфигурационных Единиц (CI);
- причина изменения, включая обоснование и ожидаемый бизнес-результат;
- текущая и новая версия изменяемой Конфигурационной Единицы;
- имя, адрес и номер телефона лица, направляющего Запрос;
- дата подачи;
- предварительная оценка необходимых ресурсов и времени.

7.4.2. Прием в обработку

После регистрации Запроса на Изменения (RFC) Управление Изменениями делает первичную проверку, нет ли среди них неясных, нелогичных, непрактичных или ненужных Запросов. Такие Запросы отклоняются с объяснением причин. Сотруднику, направившему Запрос, всегда должна быть предоставлена возможность для защиты своего Запроса.

Проведение изменения ведет за собой обновление в базе данных CMDB, например:

- изменение статуса существующей Конфигурационной Единицы;
- изменение взаимосвязи между различными Конфигурационными Единицами;
- новая Конфигурационная Единица или изменение существующей Конфигурационной Единицы;
- новый владелец или другое месторасположение Конфигурационной Единицы.

Если Запрос на Изменения (RFC) принимается в работу, в регистрационную запись изменения включается информация, необходимая для дальнейшей обработки изменения. Позднее к записи добавляется следующая информация:

- назначенный приоритет;
- оценка степени воздействия и требующихся затрат;
- категория;
- рекомендации Руководителя Процесса Управления Изменениями;
- дата и время авторизации изменения;
- запланированная дата проведения;
- план возврата к исходному состоянию;
- требования по поддержке;
- план проведения изменения;
- информация о разработчике и сотрудниках, ответственных за проведение изменения;
- фактическая дата и время проведения изменения;
- дата проведения оценки результатов;
- результаты испытания и обнаруженные проблемы;
- причины отклонения Запроса (если необходимо);
- оценка результатов.

7.4.3. Классификация

После приема Запроса на Изменения (RFC) определяются его приоритет и категория.

- **Приоритет** показывает, насколько важным является данный Запрос по сравнению с другими. Это, в свою очередь, определяется его срочностью и степенью воздействия. Если изменение касается исправления известной ошибки, код приоритета уже может быть назначен

Управлением Проблемами. Однако Управление Изменениями назначает окончательный код приоритета после рассмотрения других обрабатываемых Запросов.

- Управление Изменениями присваивает **категорию**, исходя из степени воздействия и требуемых ресурсов. Эта классификация определяет дальнейшие процедуры обработки Запроса и обозначает важность изменения.

Определение приоритета

Пример системы кодирования приоритетов:

- **Низкий приоритет** — изменение желательно, но его внедрение может быть отложено до более удобного времени (например, до следующего релиза или планового обслуживания).

- **Обычный приоритет** — нет особой срочности и высокой степени воздействия, но изменение не следует откладывать. На совещании Консультативного комитета (САВ) при выделении ресурсов изменению присваивается обычный приоритет.

- **Высокий приоритет** — изменение касается серьезной ошибки, затрагивающей ряд пользователей, или новой нетипичной ошибки, затрагивающей большую группу пользователей, или связано с другими срочными вопросами. Такому изменению на ближайшем совещании САВ присваивается высокий приоритет.

- **Наивысший приоритет** — Запрос на Изменения (RFC) касается проблемы, серьезно влияющей на важнейший для заказчиков сервис, или касается срочного изменения в ИТ (например, новой функциональности для целей бизнеса), срочного изменения законодательства или быстрых не больших изменений, не терпящих отсрочки¹. Изменения с таким приоритетом классифицируются как «срочные». Для срочных изменений обычные процедуры не используются, так как необходимые ресурсы предоставляются незамедлительно. Может потребоваться проведение срочного совещания Консультативного комитета (САВ) или Руководящего комитета ИТ². Специально для этих целей в компании должен быть сформирован Комитет по срочным изменениям (САВ/ЕС)³ с полномочиями для принятия экстренных решений. Все принятые ранее планы могут быть отложены или прерваны.

Эти коды могут быть представлены в цифрах, например: низкий приоритет = 1 / наивысший приоритет = 4.

Определение категории

Категории определяются в рамках Процесса Управления Изменениями, в случае необходимости с участием Консультативного комитета (САВ), который определяем степень воздействия изменения и требования, предъявляемые им к ИТ-организации (в первую очередь, выделение ресурсов). Примеры категорий:

- **Низкая степень воздействия** — изменение, требующее выполнения небольшого объема работ. Руководитель Процесса Управления Изменениями может авторизовать эти изменения без привлечения Консультативного комитета (САВ).

- **Существенная степень воздействия** — изменение, требующее значительных усилий и оказывающее существенное воздействие на ИТ-услуги. Эти изменения обсуждаются на совещании Консультативного комитета (САВ) для определения необходимых усилий (ресурсов и др.) и потенциального воздействия. Перед совещанием членам Консультативного комитета (САВ) и, возможно, специалистам и разработчикам направляется соответствующая документация.

- **Наивысшая степень воздействия** — изменение, требующее значительных усилий. Руководителю Процесса необходимо предварительно получить авторизацию на выполнение изменения от руководства ИТ или Руководящего комитета ИТ, после чего изменение представляется на рассмотрение Консультативного комитета (САВ).

Эти коды могут быть представлены в цифрах, например: низкая степень=1/ высшая степень = 3

¹ Quick fix.

² IT Steering Committee

³ Emergency Committee.

Большинство изменений относятся к двум первым категориям. В дополнение к классификации должны быть также определены группы, участвующие в работе над техническим решением, и услуги, затрагиваемые изменением.

7.4.4. Планирование

В рамках процесса осуществляется планирование изменений на основе графика, называемого *Согласованным планом изменений*¹ (FSC). План FSC содержит подробную информацию обо всех утвержденных изменениях и их планировании. Члены Консультативного комитета (CAB) дают рекомендации по планированию изменений, так как необходимо учитывать наличие персонала, ресурсов, затраты, различные аспекты задействованных услуг, а также мнение заказчиков. Консультативный комитет (CAB) играет роль консультативного органа. В целом Управление Изменениями имеет делегированные полномочия, т. к. оно действует от лица руководства ИТ. Возможно, что изменения наивысшей категории необходимо утверждать руководством ИТ до их представления Консультативному комитету (CAB). Утверждение изменения имеет несколько аспектов:

- **Финансовое одобрение** — анализ затрат/выгод и выделение бюджета.
- **Техническое одобрение** — оценка необходимости, возможности проведения изменения и его степени воздействия.
- **Бизнес-одобрение** — одобрение пользователями требуемой функциональности приложения и степени воздействия изменения.

Для целей эффективного планирования Управление Изменениями должно взаимодействовать с проектным офисом и другими подразделениями компании, занимающимися разработкой и внедрением изменений. Кроме того, достаточное внимание должно уделяться своевременному осведомлению пользователей о планировании изменений, возможно, в виде рассылки *Согласованного плана изменений* (FSC).

Политика проведения изменений

Изменения по разным Запросам можно объединять в одном релизе. В этом случае при неудачной реализации будет достаточно одного возврата к исходному состоянию². Такой групповой релиз должен рассматриваться как одно изменение, даже если он содержит в себе несколько изменений. Релизы могут планироваться с учетом функциональных задач, необходимых для бизнеса. Они могут охватывать аппаратные и программные средства, и их внедрение осуществляется Процессом Управления Релизами. Рекомендуется определить политику компании в этой области и информировать о ней ИТ-организацию и заказчиков (см. также «Управление Релизами»). Цель политики — оградить пользователя от ненужного беспокойства («перекапывание дороги каждую неделю»).

После консультаций с участвующими ИТ-подразделениями, Консультативный комитет (CAB) может определить регулярные периоды времени («окна») для проведения изменений, когда степень воздействия на ИТ-сервисы будет минимальной. Подходящими периодами могут быть выходные дни или нерабочее время. Таким же образом могут быть определены периоды, когда допускается минимум изменений или они вообще не допускаются, например, рабочее время или конец финансового года, когда все подразделения пользователей делают отчеты.

Совещания Консультативного комитета (CAB)

Информация о планировании изменений должна распространяться заранее до совещания CAB. Соответствующая документация и информация о пунктах повестки дня также должны рассылаться до совещания.

Повестка дня совещания CAB должна включать ряд постоянных пунктов, в том числе:

- неавторизованные изменения;

¹ Forward Schedule of Change - FSC.

² Back-out.

- Запросы на Изменения (RFC), которые должны быть оценены членами Консультативного комитета (CAB);
- авторизованные изменения, которые не были представлены на рассмотрение консультативного комитета (CAB);
- открытые и закрытые изменения;
- оценка произведенных изменений.

Оценка степени воздействия и ресурсов

При оценке необходимых ресурсов и степени воздействия изменения члены Консультативного комитета (CAB), Руководитель Процесса Управления Изменениями и другие участники (определенные Консультативным комитетом) должны учесть следующие аспекты:

- вопросы возможностей («мощности» или «емкости») подвергающихся воздействию услуг;
- надежность и возможность восстановления;
- планы по Управлению Непрерывностью ИТ-услуг;
- планы возврата к исходному состоянию;
- вопросы безопасности;
- степень воздействия изменения на другие ИТ-сервисы;
- регистрация изменения и его предварительное одобрение;
- необходимые ресурсы и затраты (поддержка и обслуживание);
- количество и наличие необходимых специалистов;
- необходимое время на весь цикл изменения;
- новые ресурсы, которые должны быть закуплены и пройти тестирование;
- степень воздействия на текущую операционную деятельность;
- какие-либо возможные конфликты с другими изменениями.

Члены Консультативного комитета (CAB) могут также дать рекомендации по определению приоритета изменения.

7.4.5. Координация

Об утвержденных изменениях сообщают соответствующим техническим специалистам, которые будут разрабатывать и внедрять эти изменения. Перед внедрением происходит этап тестирования. В разработке, испытании и внедрении утвержденных изменений важную роль может играть Процесс Управления Релизами. Большое внимание должно уделяться вопросам информирования персонала внутри компании для поддержки изменений.

Подготовка изменения¹

Не все изменения проходят отдельную фазу компоновки. Например, стандартные изменения, такие как перемещение персональных компьютеров, могут планироваться и осуществляться незамедлительно.

Компоновка может включать создание новой версии программы с новой документацией, руководствами, инсталляционными процедурами, планом возврата к исходному состоянию и аппаратными изменениями. Управление Изменениями осуществляет контроль и координацию, его поддерживают Процесс Управления Релизами и руководители линейных подразделений, которые обеспечивают предоставление необходимых ресурсов.

Процедура возврата к исходному состоянию должна разрабатываться как часть общей схемы проведения изменения на случай, если изменение не обеспечивает достижение необходимого результата. Управление Изменениями не должно одобрять проведение изменения при отсутствии

¹ Building.

процедуры возврата. Если изменение влияет на среду пользователя, должен быть составлен коммуникационный план. План внедрения изменения также составляется на стадии компоновки.

Показатели эффективности¹ демонстрируют, насколько успешно Процесс Управления Изменениями осуществляет эффективную и рациональную обработку изменений при минимальном возможном отрицательном воздействии на согласованный Уровень Услуг. Эти показатели охватывают такие параметры, как:

- количество завершенных изменений за определенный промежуток времени в разбивке по категориям;
- скорость проведения изменений; •количество отклоненных изменений; •количество инцидентов, вызванных изменениями;
- количество возвратов к исходному состоянию, связанных с проведением изменений; •затраты на произведенные изменения;
- соотношение между расчетными и фактическими затратами ресурсов и времени; •количество срочных изменений.

Тестирование

Процедура возврата к исходному состоянию, план внедрения изменения и ожидаемый результат должны проходить тщательную проверку. При этом необходимо учитывать критерии, определенные ранее консультативным комитетом (САВ). В большинстве случаев для испытаний необходима изолированная тестовая среда или лаборатория. Тестирование на ранних стадиях может производиться разработчиками, однако внедрение изменений не может осуществляться без проведения независимого тестирования. Обычно проводится два вида испытаний: приемосдаточные испытания для пользователей, при которых представители бизнес-подразделений (обычно заказчики изменения) проверяют его функциональные характеристики, и операционные (эксплуатационные) испытания², при которых независимое тестирование проводят те, кто должен поддерживать и обслуживать новую инфраструктуру. Сюда включаются также отделы технической поддержки и Служба Service Desk. Они проверяют соответствующую документацию, процедуры резервного восстановления данных (back-up) и т. д. Необходимы также четкие инструкции для мониторинга качества тестирования и документирования его результатов.

Внедрение³

Любой сотрудник соответствующего подразделения, ответственный за администрирование ИТ-инфраструктуры, может получить задание о непосредственном проведении (внедрении) изменения. Управление Изменениями гарантирует, что это является запланированным изменением. Должен существовать точный план информирования всех вовлеченных сотрудников о проведении изменения (коммуникационный план), например, пользователей, Службы Service Desk, группы администрирования сетей и т. п.

При невозможности проведения необходимого тестирования возможно внедрение изменения для небольшой пилотной группы пользователей и оценка полученных результатов перед внедрением изменения в более широком масштабе.

7.4.6. Оценка

Необходимо давать оценку произведенным изменениям, за возможным исключением стандартных изменений. При необходимости Консультативный комитет (САВ) принимает решение о проведении последующих дополнительных мероприятий. Должны быть рассмотрены следующие вопросы:

- Привело ли изменение к достижению намеченной цели?

¹ Performance indicators.

² Operational acceptance

³ Implementing

- Удовлетворены ли пользователи результатом?
- Возникали ли какие-либо побочные эффекты?
- Были ли превышены расчеты по затратам и ресурсам?

Если изменение осуществлено успешно, Запрос на Изменение (RFC) может быть закрыт. Это происходит на этапе Анализа результатов внедрения¹ (PIR), т. е. этапе оценки изменения. Если же изменение закончилось неудачно, процесс возобновляется с того места, где он вызвал сбой, с использованием нового подхода. Иногда бывает лучше сделать возврат назад и создать новый или модифицированный Запрос на Изменения (RFC). Продолжение работы с неудачным изменением часто приводит к ухудшению ситуации.

Процедуры с автоматическим отслеживанием времени гарантируют, что этап оценки изменений не будет пропущен. В зависимости от природы изменения оценку можно проводить или через несколько дней, или через несколько месяцев. Например, оценка изменения в используемом ежедневно персональном компьютере может быть совершена через несколько дней, а изменение в системе, использующейся раз в неделю, может быть сделана только через три месяца.

7.4.7. Проведение срочных изменений

Как бы хорошо ни проводилось планирование, могут быть изменения, требующие наивысшего приоритета. Срочные изменения очень важны для компании и они должны осуществляться как можно скорее. В большинстве случаев на эти изменения направляют ресурсы, предназначенные для других видов деятельности. Срочные изменения могут серьезно повлиять на запланированную работу. Следовательно, задачей является сведение к минимуму числа срочных или неожиданных изменений (с «наивысшим» приоритетом). Возможные превентивные меры включают:

- обеспечение своевременной подачи Запросов на Изменения, пока они не стали срочными.
- при исправлении ошибок, возникших в результате плохой подготовки изменений, возврат не должен заходить дальше прежней версии, то есть дальше Прежнего стабильного состояния². После возврата следует тщательно подготовить новый улучшенный план изменения.

Несмотря на указанные выше меры срочные изменения все же могут возникнуть. Они требуют процедур для срочной обработки, но с сохранением общего контроля со стороны Процесса Управления Изменениями. В случае возникновения такой ситуации Руководитель Процесса Управления Изменениями может организовать чрезвычайное совещание комитета САВ/ЕС. Если для этого нет времени или если Запрос поступил в нерабочее время, должен существовать альтернативный способ получения авторизации изменения. Это не обязательно должна быть встреча «лицом к лицу», вместо нее можно провести телефонную конференцию.

Пример этого был упомянут в главе по Управлению Инцидентами, когда экстренный ремонт может быть предложен для разрешения серьезного инцидента. Если дело обстоит очень плохо и отсрочка неприемлема, необходимо следовать процедуре обработки срочного Запроса на Изменение.

Возможна также нехватка времени для проведения нормального тестирования. Например, рабочая станция управляет большой машиной, которая смешивает крахмал для приготовления таблеток в фармацевтическом производстве. Если рабочая станция не будет исправлена в течение часа, крахмал затвердеет, и для его удаления вручную, с помощью молотка и зубила, потребуются работа двух человек в течение двух недель. В это время компания будет терпеть убытки в тысячи долларов за час, так как препараты не будут производиться. При такой ситуации Руководитель Процесса Управления Изменениями должен оценить риски и принять решение о проведении изменения. После этого должны быть пройдены все необходимые этапы нормального процесса для гарантии того, что все пропущенные испытания теперь проведены, вся информация обновлена (произведена регистрация изменений в базе данных CMDB) и что все изменения отслеживаются.

7.5 Контроль процесса

¹ Post Implementation Review - PIR

² Previous Trusted State.

7.5.1 Отчеты для руководства

Задачей Процесса Управления Изменениями является достижение баланса между гибкостью и стабильностью. Для характеристики текущей ситуации в организации могут быть использованы следующие отчеты:

- количество проведенных изменений за определенный период времени (всего и по категориям Конфигурационных Единиц);
- перечень причин изменений и перечень Запросов на Изменения;
- количество успешно внедренных изменений;
- количество возвратов к исходному состоянию и их причины;
- количество инцидентов, связанных с проведенными изменениями;
- графики и анализ тенденций за соответствующие периоды.

Показатели эффективности¹ определяют, насколько успешно Процесс Управления Изменениями осуществляет эффективную² и рациональную³ обработку изменений при минимальном отрицательном воздействии на согласованный Уровень Услуг. Эти показатели могут быть следующими:

- количество изменений, завершенных за единицу времени, по категориям;
- скорость проведения изменений;
- количество отклоненных изменений;
- количество инцидентов, вызванных изменениями;
- количество возвратов к исходному состоянию, связанных с изменениями;
- затраты на проведенные изменения;
- количество изменений, осуществленных в рамках расчетных затрат ресурсов и времени.

7.6. Затраты и проблемы

7.6.1. Затраты

▪ **Затраты на персонал** — в большинстве случаев уже имеется персонал, занимающийся координацией изменений. Однако для выполнения задач Руководителя Процесса Управления Изменениями и организации работы Консультативного комитета по изменениям (САВ) возможны дополнительные расходы на персонал. Во многих случаях Управление Изменениями вводится для повышения качества услуг, и возникшие дополнительные расходы рассматриваются как расходы на качество. После успешного запуска процесса расходы на координацию изменений компенсируются уменьшением расходов на разрешение инцидентов и проблем.

▪ **Затраты на инструментальные средства** — расходы на аппаратное и программное обеспечение должны определяться заранее. Часто при внедрении нескольких процессов закупается общее инструментальное средство для Процессов Управления Изменениями, Проблемами, Конфигурациями и Инцидентами. При работе в сложной ИТ-среде почти невозможно контролировать эти процессы без такого инструментального средства.

7.6.2. Проблемы

При внедрении Процесса Управления Изменениями возможно появление следующих проблем:

Работа без средств автоматизации слишком трудоемка, она будет создавать много проблем.

▪ Возможно сопротивление всеохватывающему Процессу Управления Изменениями, осуществляющему мониторинг всех аспектов ИТ-инфраструктуры. В этом случае необходимо обучение персонала, который должен осознать, что все компоненты ИТ-инфраструктуры могут оказывать значительное влияние друг на друга, и что реализуемые изменения Конфигурации требуют общей координации.

¹ Performance indicators.

² Effective.

³ Efficient.

- Возможны попытки проведения изменений в обход согласованных процедур. Абсолютно необходимо, чтобы такие попытки встречали соответствующую реакцию со стороны компании. Целостность Процесса Управления Изменениями зависит от полного соответствия процедурам. Претензии сотрудников и предложения по усовершенствованию Процесса Управления Изменениями должны пониматься и приветствоваться, однако неподчинение необходимо решительно пресекать, иначе весь процесс будет поставлен под угрозу.

- Другие способы обеспечения исполнения процедур по Управлению Изменениями включают:

- проведение регулярного аудита, возможно, независимым инспектором, для оценки соответствия процедурам Управления Изменениями;

- осуществление контроля со стороны руководства над внутренним и внешним обслуживающим персоналом и разработчиками;

- обеспечение контроля за всеми Конфигурационными Единицами и версиями программ путем защиты базы данных CMDB и организации регулярного аудита Конфигураций в рамках Процесса Управления Конфигурациями;

- предоставление информации из Управления Инцидентами о фактах доступа пользователей к аппаратному и программному обеспечению, не отраженного в CMDB;

- включение необходимых условий и процедур в контракты с внешними поставщиками;

- назначение на должность Руководителя Процесса Управления Изменениями сотрудника с обширным опытом и достаточными бизнес- (что часто недооценивается) и техническими знаниями. Правильный выбор претендента на эту должность имеет критически важное значение, это не должно упускаться из виду, как часто бывает.

7.6.3. Предложения

Некоторые проблемы могут быть решены за счет реализации следующих предложений:

- обеспечить, чтобы каждое изменение проходило всю процедуру обработки.

- наладить контакт со всем ИТ-персоналом и всеми поставщиками, чтобы гарантировать их понимание Процесса Управления Изменениями и отказ от попыток проведения изменений без координации;

- обеспечить постоянное проведение окончательной оценки изменений (Анализ результатов внедрения - PIR);

- организовать взаимодействие с Управлением Конфигурациями для гарантированного ввода изменений Конфигурационных Единиц в базу данных CMDB.

Глава 8

Управление Релизами

8.1. Введение

С повышением зависимости организаций от ИТ-процессов все большее значение приобретает их эффективный мониторинг и защита. С ростом количества изменений возрастает и потребность в контроле над процессом проведения изменений.

Изменения ИТ-инфраструктуры происходят в сложной распределенной среде. В современных приложениях клиент/сервер это часто отражается как на клиентской части, так и на серверной. В таких случаях запуск и внедрение новых версий программных и аппаратных средств требует тщательного планирования. Релизом называется набор новых и/или измененных Конфигурационных Единиц, которые вместе испытываются и внедряются в рабочую среду. Релиз определяется Запросом на Изменения (RFC), для исполнения которого он вводится в работу. В Процессе Управления Релизами используется плановый проектный подход к проведению изменений в ИТ-услугах, и он затрагивает все, как технические, так и нетехнические аспекты изменений.

Задачей Процесса Управления Релизами является обеспечение качества рабочей среды¹ за счет использования формальных процедур и проверок при вводе в работу новых версий. В отличие от Управления Изменениями, занимающегося верификацией, Процесс Управления Релизами занимается внедрением. Управление Релизами осуществляется в тесном контакте с Управлением Конфигурациями и Управлением Изменениями, что гарантирует обновление единой базы CMDB с учетом каждого нового релиза. Управление Релизами также обеспечивает обновление содержания релизов (программных кодов) в Библиотеке эталонного программного обеспечения² DSL. С помощью базы CMDB также отслеживаются спецификации аппаратных средств, руководства по установке и сетевые конфигурации. Запас аппаратных средств, в частности стандартизованные базовые конфигурации, хранится на Складе эталонного аппаратного обеспечения³ DHS. Однако, в первую очередь объектом Процесса Управления Релизами является программное обеспечение.

В больших проектах Процесс Управления Релизами должен включаться в общий план проекта как его составная часть для обеспечения достаточного финансирования работы процесса. Определенная часть ежегодного бюджета может быть выделена на повседневные работы, такие как незначительные изменения. Расходы, возникающие при запуске процесса, не столь значительны по сравнению с потенциальными потерями, вызванными недостатками в планировании и контроле за программными и аппаратными средствами, к которым можно отнести следующие:

- большие перерывы в работе из-за плохого планирования выпуска релизов;
- дублирование работ из-за наличия копий различных версий;
- неэффективное использование ресурсов из-за отсутствия информации об их местонахождении;
- потеря исходных файлов, приводящая к повторной закупке программ;
- отсутствие защиты от вирусов, приводящее к необходимости «лечения» всей сети.

8.1.1. Основные понятия

Релизы

Релизы содержат одно или несколько авторизованных изменений. Они могут классифицироваться в первую очередь по уровню релиза. Часто релизы разделяют на:

- **Значительные релизы** — крупномасштабное развертывание новых аппаратных и программных средств, обычно со значительно расширенными функциональными возможностями.

¹ Production environment.

² . Definitive Software Library - DSL

³ Definitive Hardware Store - DHS.

Такие релизы часто помогают в устранении ряда известных ошибок, включая известные обходные решения¹ и быстрые исправления².

- **Малые программные релизы и модернизация аппаратного обеспечения (апгрейды)**³ — эти релизы обычно представляют собой незначительные усовершенствования и исправления известных ошибок. Среди них могут быть такие, которые внедрялись ранее в виде срочных исправлений и теперь окончательно проработаны и включены в данный релиз. За счет такого релиза обеспечивается обновление «Прежнего стабильного состояния»⁴, являющегося отправной точкой для всех испытаний.

- **Срочные исправления** — обычно внедряются как быстрые исправления проблем и известных ошибок.

Релизные единицы

В отношении аппаратного обеспечения вопросы возникают только при полной замене ПК или при отдельной замене плат и дисководов жестких дисков (или даже оперативной памяти и процессоров). Для программного обеспечения изменения возможны на уровне системы, комплекса, программы или модуля. Хорошим примером может быть библиотека DLL (Dynamic Link Library) в среде Windows, часто используемая несколькими программами. Иногда в составе пакета поставляется новая версия DLL, что может потребовать нового тестирования и переустановки всех других программных пакетов. В данном процессе также прорабатывается принцип минимального содержания релиза.

Идентификация релизов

Копии программ могут распространяться из Библиотеки DSL по соответствующим средам:

- **Среда разработки** — разработка новых версий может вестись на основе более ранних версий из Библиотеки DSL. С каждой новой версией увеличивается ее номер. Изменение программного обеспечения возможно только в среде разработки.

- **Среда испытаний** — среда для тестирования версий. Часто тестирование разделяют на технические испытания разработчиками, функциональные испытания пользователями, испытания внедрения компоновщиками релизов и, возможно, окончательные приемочные испытания пользователями и руководством.

- **Рабочая среда** — активная среда, где информационные системы доступны для пользователей.

- **Архив** — служит для хранения старых версий программных единиц, которые больше не используются.

Так как возможно использование нескольких релизов, им присваиваются уникальные идентификаторы. В идентификационном номере релиза должна быть ссылка на соответствующую Конфигурационную Единицу, и он должен включать номер версии из двух или более цифр, например:

- **Значительные релизы** — система расчета зарплаты v.1, v.2, v.3 и т. п.

- **Малые релизы** — система расчета зарплаты v.1.1, v.1.2, v.1.3 и т. п.

- **Релизы** — срочные исправления — система расчета зарплаты v.1. 1.1, v.1. 1.2, v.1. 1.3 и т. п.

На рис. 8.1 показаны тестирование и возможные модификации каждой новой версии перед ее выпуском. Старая версия архивируется как часть запуска нового релиза на случай возможного возврата.

На рис. 8.2 показан возврат.

¹ Work-arounds.

² Quick fixes

³ Upgrades.

⁴ Previous Trusted State

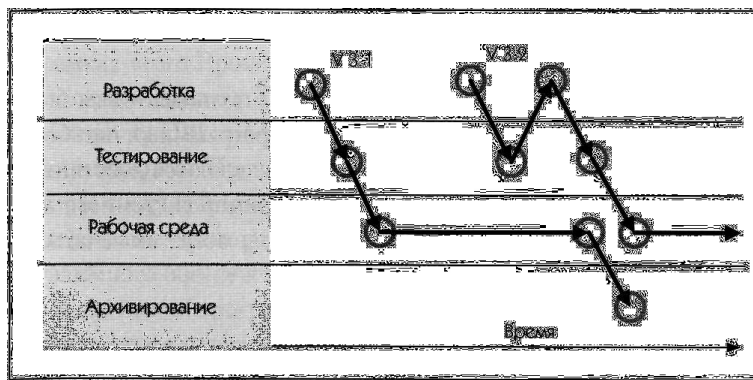


Рис. 8.1. Выпуск версии в Процессе Управления Релизами

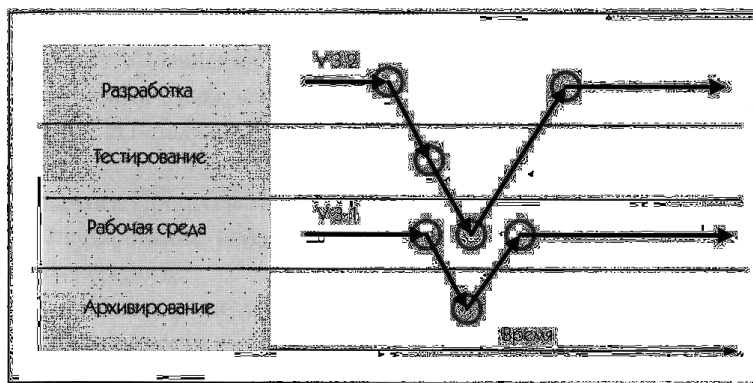


Рис. 8.2. Возврат в Процессе Управления Релизами

Типы релизов

Должна быть произведена оценка, какое количество изменений может быть разработано, испытано и внедрено за определенный период времени. Может оказаться, что пакетный релиз, представляющий собой комбинацию нескольких изменений для одного развертывания, может быть слишком сложным для безопасного внедрения.

Быстрая разработка и продвижение на рынок новых версий аппаратного и программного обеспечения может привести к тому, что релиз может устареть до его внедрения. С другой стороны, частые изменения могут оказать отрицательное воздействие на предоставление услуг.

В рамках Процесса Управления Изменениями принимается решение о количестве изменений, которое может быть включено в релиз, и о способе его развертывания. Возможен выбор одного из следующих вариантов:

- **Дельта-релиз** — в дельта-релиз включаются только измененные аппаратные и программные средства. Это часто связано с экстренными и быстрыми исправлениями. Недостатком этого типа релизов является то, что часто невозможно проверить все связи с остальной частью среды, в результате чего не удаляются модули, к которым программа больше не обращается. Дельта-релиз удобен в случае, если программное обеспечение может быть изолировано от остальной части ИТ-среды. Преимуществом дельта-релиза является то, что для создания тестовой среды требуется меньше усилий.

- **Полный релиз** — при полном релизе идет распространение полного комплекта ПО, включая неизмененные модули. Такой подход предпочтителен в случаях, когда точно не известно, что изменено в программном обеспечении. Более тщательные испытания программных и аппаратных средств обеспечивают в этом случае меньшее число инцидентов после внедрения. При подготовке полного релиза легче определить, достигается ли запланированный уровень производительности. Преимуществом полного релиза является возможность одновременного внедрения нескольких изменений. Подготовка облегчается благодаря возможности использования стандартных сценариев инсталляции¹.

Также при инсталляции может быть «очищена» программная среда. Однако полный релиз требует большей подготовки и ресурсов, чем дельта-релиз.

- **Пакетный релиз** — пакетный релиз, или комплект релизов, обеспечивает пользователям более длительные периоды стабильной работы. Исправление незначительных

¹ Standard installation scripts.

программных ошибок, с которыми пользователи могут мириться, и внедрение новых функций часто являются действиями, которые можно эффективно объединить. Так же плановые апгрейды, например системного программного обеспечения и офисных приложений от внешних разработчиков, могут включаться в пакетные релизы.

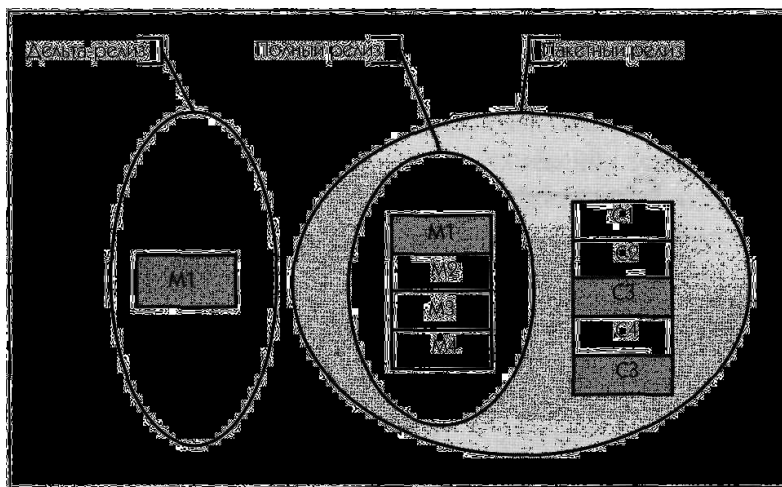


Рис. 8.3. Типы релизов

Библиотека эталонного программного обеспечения¹ (DSL)

Библиотека эталонного программного обеспечения (DSL) — это надежное хранилище для эталонных авторизованных версий (мастер-копий) всех Конфигурационных Единиц программного обеспечения. Физически библиотека DSL может находиться в разных местах и состоять из нескольких надежных хранилищ и огнестойчивых сейфов для носителей информации. Управление Релизами начинает контролировать жизненный цикл программ с момента их включения в библиотеку DSL. Релизы конфигурируются из известного надежного программного обеспечения, хранящегося в DSL. После этого разрабатываются инсталляционные скрипты², а в децентрализованной среде могут быть записаны соответствующие компакт-диски.

В библиотеке DSL может храниться несколько версий одного и того же программного обеспечения, включая архивные версии, документацию и исходные коды. Поэтому необходимо создание резервных копий³ Библиотеки DSL, поскольку она содержит не только текущую версию программного обеспечения, но и копии на случай возврата к прежней версии. При наличии в компании нескольких территориальных объектов с локальным руководством, на каждом из них должна быть копия Библиотеки DSL на случай развертывания программного обеспечения.

Склад эталонного аппаратного обеспечения⁴ (DHS)

Склад эталонного аппаратного обеспечения предназначен для хранения запасных аппаратных средств. Это запасные компоненты и узлы, состояние которых поддерживается на том же уровне, что и у соответствующих им компонентов в активной среде. Аппаратные средства со склада DHS используются для замены или ремонта аналогичных Конфигураций в ИТ-инфраструктуре. Информация о составе этих Конфигураций должна содержаться в базе CMDB.

Конфигурационная База Данных (CMDB)

В рамках всего Процесса Управления Релизами рекомендуется проверять информацию о Конфигурационных Единицах в базе CMDB. Как только версии программного обеспечения добавляются в Библиотеку DSL, а версии аппаратных средств - на Склад DHS, производится

¹ Definitive Software Library - DSL.

² Installation scripts

³ Back-up

⁴ Definitive Hardware Store - DHS.

обновление CMDB. Для поддержки Процессы Управления Релизами база данных CMDB должна содержать информацию по следующим вопросам:

- содержание запланированных релизов, включая Конфигурационные Единицы аппаратного и программного обеспечения со ссылкой на исходный Запрос на Изменения (RFC);
- аппаратные и программные Конфигурационные Единицы, на которые может повлиять релиз;
- данные о физическом местонахождении аппаратных средств, имеющих отношение к релизу.

8.2. Цель процесса

Процесс Управления Релизами занимается управлением и распространением (дистрибуцией) используемых в рабочей среде версий программного и аппаратного обеспечения, находящихся на поддержке ИТ-подразделения для обеспечения необходимого уровня услуг.

Задачами Процессы Управления Релизами являются:

- Планирование, координация и внедрение (или организация внедрения) программных и аппаратных средств.
- Разработка и внедрение рациональных¹ процедур для распространения и инсталляции изменений в ИТ-системах.
- Обеспечение отслеживаемости и безопасности программных и аппаратных средств, подвергшихся изменениям, и гарантирование того, что в рабочей среде находятся только корректные, авторизованные и тестированные версии.
- Коммуникации и оповещение пользователей, учет их ожиданий при планировании и развертывании новых релизов.
- Определение состава релизов и планирование их развертывания совместно с Процессом Управления Изменениями.
- Внедрение новых версий программных и аппаратных средств в рабочую инфраструктуру под контролем Управления Изменениями и при поддержке Управления Конфигурациями. Релиз может включать любое количество Конфигурационных Единиц, а также не только программные и аппаратные средства, но и документацию, например, отчеты, планы, руководства по поддержке.
- Обеспечение сохранности оригинальных копий программ в Библиотеке эталонного программного обеспечения (DSL) и регулярного обновления базы данных CMDB; то же касается аппаратных средств на Складе DHS.

8.2.1. Преимущества использования процесса

Вместе с эффективными Процессами Управления Конфигурациями и Управления Изменениями Процесс Управления Релизами способствует тому, чтобы:

- Использовалось программное и аппаратное обеспечение высокого качества, которое разрабатывалось и тестировалось с проведением процедур контроля качества.
- Сводилась к минимуму возможность возникновения ошибок в программно-аппаратных комплексах, или ошибок выпуска некорректных версий.
- Бизнес-подразделения внимательно контролировали инвестиции в программное обеспечение, от которых во многом зависит бизнес.
- Уменьшалось общее количество отдельно взятых внедрений, и проводились серьезные испытания каждого внедрения.
- Уменьшалась опасность возникновения инцидентов и известных ошибок за счет тестирования и контроля внедрения.
- Пользователи больше привлекались к участию в тестировании релизов.

- Заранее публиковалась программа ввода релизов для улучшения координации ожиданий пользователей с политикой и практикой появления новых релизов.
- Для целей бизнеса существовали структуры централизованного проектирования и компоновки программных и аппаратных средств или структуры для их закупки с последующим распространением по пользователям.
- Бизнес-подразделения могли стандартизировать версии программного и аппаратного обеспечения в своих подразделениях для облегчения их поддержки.
- Уменьшалась опасность использования пиратских программ, а также опасность возникновения инцидентов и проблем из-за интегрирования в активную среду дефектных или зараженных вирусом версий программного и аппаратного обеспечения.
- Облегчалось обнаружение неавторизованных копий и некорректных версий.

8.3. Процесс

Процесс Управления Релизами состоит из следующих видов деятельности:

- разработка политики в отношении релизов и их планирование;
- компоновка и конфигурирование релизов;
- тестирование и приемка релизов;
- планирование развертывания релизов;
- оповещение, подготовка и обучение;
- распространение и инсталляция релизов.

В действительности эти виды деятельности не располагаются в хронологическом порядке. Определение политики и планирование релизов могут проводиться раз в полгода или в год, в то время как другие действия могут проводиться ежедневно.

Рис. 8.4. Управление Релизами



Успешное проведение Управления Релизами зависит от входной информации, поступающей из других процессов ИТIL, и от взаимодействия с этими процессами (рис. 8.4). Главными являются интерфейсы со следующими процессами.

8.3.1. Управление Конфигурациями

Управление Конфигурациями отвечает за регистрацию доступных версий программного и аппаратного обеспечения в базе данных CMDB в качестве Базисных Конфигураций. Программы, включаемые в Библиотеку DSL, и аппаратные средства для DHS регистрируются в CMDB с согласованным уровнем детализации. Мониторинг статуса, выполняемый Процессом Управления Конфигурациями, отражает статус каждой Конфигурационной Единицы, например, «В активном использовании», «В разработке», «В тестировании», «В запасе» или «В архиве».

8.3.2. Управление Изменениями

Деятельность по распространению (тиражированию) релизов контролируется Процессом Управления Изменениями. Кроме того, Управление Изменениями гарантирует, чтобы было проведено адекватное тестирование релизов. Управление Изменениями также принимает решение о количестве изменений, которые могут быть скомбинированы в одном релизе. Управление Изменениями определяет процедуры, обеспечивающие авторизацию изменений, включая анализ степени воздействия и анализ необходимых ресурсов. В большинстве случаев Руководитель Процесса Управления Релизами несет ответственность за внедрение программных и аппаратных изменений и он обычно участвует в работе Консультативного комитета по изменениям.

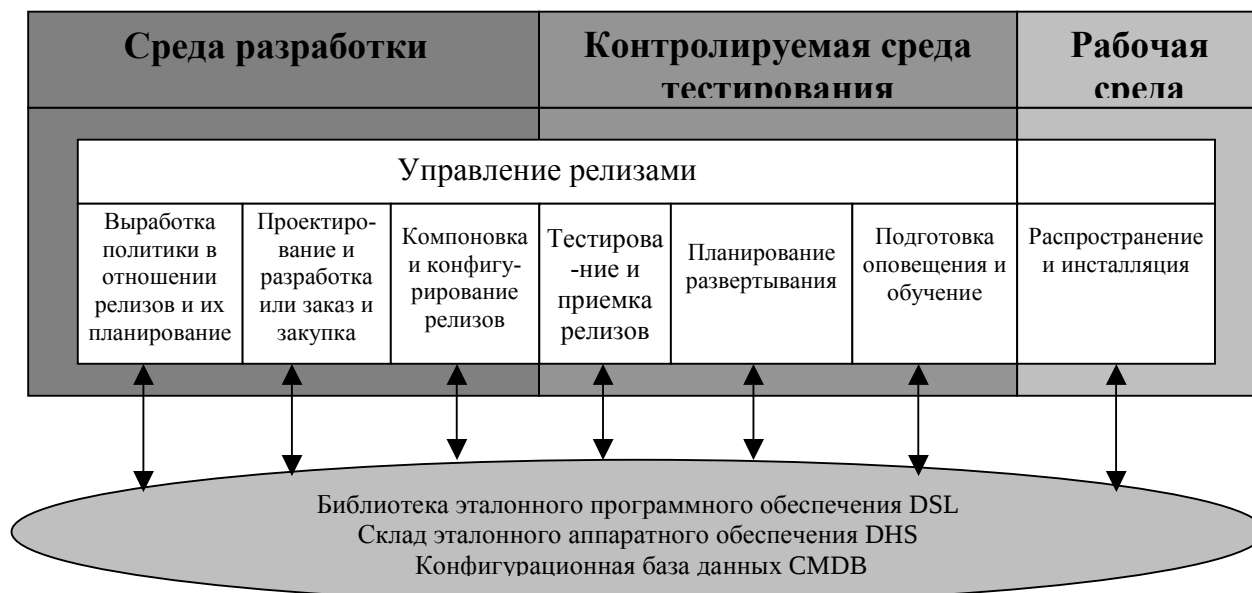
8.3.3. Управление Уровнем Услуг

ИТ-сервис обычно включает в себя инфраструктурное аппаратное обеспечение вместе со стандартным или разработанным собственными силами программным обеспечением. Управление Релизами отвечает за ввод в работу программных и аппаратных средств и отслеживает соглашения о доступности программных средств, заключенные в рамках Процесса Управления Уровнем Услуг.

8.3.4. Виды деятельности

На рис. 8.5 показаны виды деятельности в рамках Процесса Управления Релизами и их связи с жизненным циклом изменения.

Рис. 8.5. Виды деятельности по Управлению Релизами (источник: OGC)



8.4. Виды деятельности

8.4.1. Выработка политики в отношении релизов и планирование

Руководитель Процесса Управления Релизами разрабатывает политику в отношении релизов, определяя когда и каким образом производится конфигурирование релизов. Значительные релизы могут планироваться заранее, одновременно с присвоением номера версии, чтобы в определенные моменты времени можно было рассмотреть возможность внесения изменений.

Руководитель Процесса Управления Релизами также определяет, на каком уровне Конфигурационные Единицы могут распространяться независимо друг от друга (релизные единицы). Это зависит от:

- Потенциального воздействия релиза на другие компоненты.
- Количества человеко-часов и времени на компоновку и тестирование отдельных изменений, в сравнении с усилиями, необходимыми для их объединения и одновременного внедрения.
- Трудности инсталляции на местах пользователей. Возможно, что инсталлировать полную программу легче благодаря наличию для этого стандартных методов.
- Сложности взаимосвязей между новым программным и аппаратным обеспечением и остальной частью ИТ-инфраструктуры - чем легче изолировать программные или аппаратные средства, тем легче их тестировать.

Перед планированием релиза необходимо собрать информацию о жизненном цикле внедряемого продукта, а также обо всех подготовленных к сдаче в рамках данного релиза продуктах, описании соответствующих ИТ-услуг и их уровней и данные об авторизации соответствующих Запросов на Изменения (RFC) и т. д. При планировании релиза рассматриваются следующие вопросы:

- координация содержания релиза;
- разработка графика ввода релиза;
- согласование графика, территориальных объектов, на которых произойдет распространение релиза, и организационных единиц;
- посещение объектов для определения реально используемых аппаратных и программных средств;
- разработка плана оповещения (коммуникаций);
- согласование ролей и ответственностей;
- получение подробных коммерческих предложений и переговоры с поставщиками о новых аппаратных и программных средствах, а также услугах по их инсталляции;
- разработка планов на случай возврата к исходному состоянию;
- разработка плана обеспечения качества релиза;
- планирование приемки релиза руководством и пользователями.

Результаты этой деятельности представляют собой часть плана проведения изменения и включают планы релиза, планы тестирования и критерии приемки.

8.4.2. Проектирование, компоновка и конфигурирование

Рекомендуется выработать стандартные процедуры проектирования, компоновки и конфигурирования релизов. Основой релизов могут быть наборы компонентов (Конфигурационных Единиц — CI), разработанные внутри организации или закупленные у третьей стороны и прошедшие этап конфигурирования. Руководства по инсталляции и конфигурированию релизов должны рассматриваться как часть релиза и в качестве Конфигурационных Единиц должны включаться в число объектов, находящихся под контролем Процессов Управления Изменениями и Управления Конфигурациями.

Перед инсталляцией на месте рекомендуется настроить и протестировать все аппаратное и программное обеспечение в «лабораторных условиях». Компоненты программных и аппаратных средств необходимо тщательно конфигурировать и зарегистрировать, чтобы обеспечить возможность их многократного воспроизведения. Необходимо разработать рабочие инструкции таким образом, чтобы каждый раз воспроизводился один и тот же набор компонентов. Часто в резерве имеются стандартизированные аппаратные средства, которые используются только для компилирования или создания образов ПО¹. Для надежности желательно, чтобы эта часть процесса была автоматизирована. Необходимые для этого программные и аппаратные средства также попадают в сферу действия Процесса Управления Релизами. В среде разработки программ такая деятельность называется Управлением Компонентом² и входит в зону ответственности Управления Релизами.

План возврата к исходному состоянию

В плане возврата к исходному состоянию на уровне релиза в целом определяются действия, необходимые для восстановления услуг в случае сбоя во время внедрения (имплементации) релиза. Ответственность за разработку планов возврата несет Процесс Управления Изменениями, но Управление Релизами должно оказывать в этом помощь для обеспечения практической реализуемости этих планов. В частности, при внедрении пакетного релиза, объединяющего несколько Запросов на Изменения (RFC), может возникнуть необходимость координации различных планов возврата для этого релиза. Если возникает сбой Полного релиза или Дельта-релиза, рекомендуется свернуть релиз полностью до Прежнего стабильного состояния³. На случай невозможности полного сворачивания релиза должны существовать Планы восстановления на случай чрезвычайных обстоятельств⁴ для возобновления предоставления услуг.

Требования плана возврата к исходному состоянию, такие как создание резервных копий и обеспечение запасного сервера, рекомендуется выполнять заранее. В случаях, если внедрение может занять больше времени, чем предполагается, и если задержка может поставить под угрозу нормальное предоставление услуг, в план возврата должен включаться крайний срок, определяющий время приведения в действие плана возврата. Это требуется для своевременного возобновления услуг (например, не позднее 7:00 в понедельник). План возврата к исходному состоянию должен включаться в анализ рисков изменения и должен быть одобрен пользователями.

Реальная компоновка релиза может включать компилирование и связывание программных модулей, или наполнение баз данных тестовыми данными, или такими данными, как таблицы почтовых индексов, налоговых ставок, часовых поясов и валютных курсов, а также информацией о пользователях. Часто это выполняется автоматизированными инсталляционными скриптами⁵, хранящимися в Библиотеке DSL вместе с планами возврата. Полные релизы должны отражаться в базе CMDB как Стандартные Конфигурации для облегчения конфигурирования в будущем. Планы тестирования должны включать тестирование и приемку по качеству программного и аппаратного обеспечения, процедур, инструкций по операционной деятельности и сценариев (скриптов) развертывания⁶ перед выходом релиза и, возможно, оценочные испытания после внедрения релиза. Должно также проводиться тестирование инсталляционных скриптов. Для этого требуется следующая информация:

- определение релиза;
- график ввода релиза;
- инструкции по конфигурированию и компоновке релиза;

¹ Creating images.

² Build Management.

³ Previous Trusted State.

⁴ Disaster Recovery Plans.

⁵ Installation scripts.

⁶ Rollout scripts. Т. е. как был определен релиз.

- описание позиций, требующих приобретения или лицензирования, с приложением графиков закупки;
- автоматизированные инсталляционные скрипты и планы тестирования;
- исходные копии кодов программ для включения в библиотеку DSL;
- планы возврата к исходному состоянию.

8.4.3. Тестирование и приемка релиза

Наиболее частой причиной неудовлетворительного внедрения изменений и релизов является неадекватность тестирования. Для предотвращения этого перед внедрением релиза должно проводиться функциональное тестирование представителями пользователей и операционное (эксплуатационное) тестирование персоналом ИТ, оценивающим технические характеристики, функциональность, операционные (эксплуатационные) аспекты, производительность и интеграцию с остальной частью инфраструктуры. Также должны тестироваться инсталляционные скрипты, процедуры возврата и любые изменения процедур управления. Формальная приемка каждого этапа должна быть представлена в Процессе Управления Изменениями. Последним этапом является утверждение внедрения релиза.

Перед тем, как Процесс Управления Релизами начнет развертывание релиза, Процесс Управления Изменениями должен организовать формальную приемку релиза пользователями и его окончательную сдачу разработчиками.

Релизы должны приниматься в контролируемой тестовой среде, состоящей из Базовых Конфигураций, которые должны быть подробно описаны в ходе определения релиза. Соответствующие Базовые Конфигурации должны быть зарегистрированы в CMDB. Если релиз не принимается, он возвращается в Процесс Управления Изменениями.

Результатами деятельности по тестированию и приемке релиза являются:

- протестированные процедуры инсталляции;
- протестированные компоненты релиза;
- известные ошибки и недостатки релиза;
- результаты тестирования;
- документация для управления и поддержки;
- перечень систем, подвергающихся воздействию;
- операционные (эксплуатационные) инструкции¹ и средства диагностики;
- планы на случай непредвиденных ситуаций и протестированные планы возврата;
- программы обучения персонала, руководителей и пользователей;
- подписанные приемо-сдаточные документы;
- авторизация из Процесса Управления Изменениями для выполнения релиза.

8.4.4. Планирование внедрения

Составленный на предыдущих этапах план теперь дополняется информацией о действиях по внедрению.

Планирование развертывания релиза включает:

- составление графика, а также перечня задач и требуемых людских ресурсов;
- составление перечня инсталлируемых и снимаемых с использования Конфигурационных Единиц, с указанием способа вывода из операционной среды;
- составление плана действий для каждого территориального объекта с учетом запаса времени на развертывание и часовых поясов, если речь идет о географически распределенных организациях;
- рассылку уведомлений о релизе и другие контакты с вовлеченными сторонами;

¹ Operating instructions

- составление планов закупки аппаратного и программного обеспечения;
- закупку, размещение на хранение, определение и регистрацию всех новых СИ для данного релиза в базе CMDB;
- планирование встреч с руководством, управляющими подразделениями, персоналом по Управлению Изменениями и представителями пользователей¹.

Существует несколько способов осуществления развертывания:

- полное развертывание релиза - подход «большого скачка»;
- поэтапное развертывание релиза, включающее несколько разновидностей:
 - функциональное наращивание, когда все пользователи получают одновременно новые элементы функциональности;
 - наращивание по объектам, когда развертывание ведется от одной группы пользователей к другой
 - эволюционное развертывание с поэтапным расширением функциональности.

8.4.5. Оповещение, подготовка и обучение

Персонал, находящийся в контакте с заказчиками (Служба Service Desk и Управление Взаимоотношениями с Заказчиками — CRM), операционный (обслуживающий) персонал и представители пользователей должны быть в курсе планов внедрения и его возможных последствий для повседневной деятельности. Для этого можно организовать совместное обучение, сотрудничество и совместное участие в приемке релиза. Необходимо согласовать распределение ответственностей, с соответствующим уведомлением каждого. При поэтапном развертывании релиза пользователи должны: быть проинформированы о планах и времени, когда для них будут доступны новые функции.

Необходимо заранее информировать весь задействованный персонал об изменениях в Соглашениях об Уровне Услуг (SLA), Операционных Соглашениях об Уровне Услуг (OLA) и Внешних Договорах (UC).

8.4.6. Распространение релизов и инсталляция

Управление Релизами осуществляет мониторинг процессов логистики/материально-технического обеспечения по закупке, хранению, транспортировке, поставке и передаче программного и аппаратного обеспечения. Этот процесс поддерживается процедурами, регистрационными записями и такими сопроводительными документами, как упаковочные листы, что необходимо для предоставления достоверной информации в Процесс Управления Конфигурациями. Склады аппаратного и программного обеспечения должны быть надежными и доступными только для авторизованного персонала.

Для распространения и инсталляции программного обеспечения рекомендуется, по возможности использовать автоматизированные инструментальные средства. Это позволит сократить время, необходимое для распространения ПО, и повысить качество при сокращении затрат на ресурсы. Часто такие инструментальные средства также облегчают проверку успешности инсталляции. Перед началом любой инсталляции необходимо проверить, удовлетворяет ли среда, где предполагается внедрение релиза, необходимым требованиям, таким как достаточное дисковое пространство, безопасность, требованиям к окружающей среде или ограничениям эксплуатационных условий, например кондиционирование воздуха, площадь помещения, источники бесперебойного питания (UPS), сете вое питание и т. п.

После инсталляции необходимо обновить информацию в базе данных CMDB для облегчения проверки лицензионных соглашений.

¹ Кроме того, для осуществления эффективной поддержки пользователей необходимо обеспечить информирование службы Service Desk о планируемом тиражировании (распространении) новых версий. — Прим. ред.

8.5. Затраты и проблемы

8.5.1. Затраты

Затраты на Процесс Управления Релизами включают:

- затраты на персонал;
- затраты на хранение в Библиотеке DSL и Складе DHS, а также на поддержку среды компоновки тестирования и распространения релизов;
- затраты на инструментальные программные средства и необходимое аппаратное обеспечение.

8.5.2. Проблемы

Возможно возникновение следующих проблем:

- **Соппротивление изменениям** - вначале возможно сопротивление персонала, привыкшего к старым привычным методам работы. Например, некоторым сотрудникам бывает трудно принять тот факт, что для проведения определенной деятельности они будут получать инструкции из другого подразделения. Для устранения таких ситуаций необходимо информировать этих сотрудников о преимуществах подхода ITIL.
- **Обход Процесса Управления Релизами** - использование неавторизованных программ может привести к распространению вирусов, отрицательно повлиять на услуги и затруднить поддержку. Поэтому в отношении персонала и пользователей, пытающихся использовать неавторизованные программы, особенно в среде РС, должны быть предприняты решительные действия.
- **Срочные исправления** - не следует действовать в обход Процесса Управления Релизами даже при необходимости срочных изменений.
- **Распространение** - при развертывании программ на нескольких объектах необходимо обеспечить их синхронизацию, для предотвращения разницы версий на разных объектах.
- **Тестирование** - без создания соответствующей тестовой среды будет трудно произвести оценку правильности новых версий или новых программ перед их развертыванием.

Глава 9

Служба Service Desk

9.1. Введение

Служба Service Desk играет важную роль в поддержке пользователей. Современная полномасштабная Служба Service Desk выполняет функции «фронт-офиса» для всей ИТ-организации и сама может решать большую часть обращений и запросов пользователей, не прибегая к помощи специалистов. Для пользователей Служба Service Desk является единой точкой контактов с ИТ-организацией, гарантирующей своевременное решение их вопроса. Другими словами, при наличии Службы Service Desk пользователям не нужно тратить время на бесконечные поиски специалистов, которые смогут решить их проблемы. Часто Служба Service Desk занимается не только обработкой внешних обращений пользователей, но и тех обращений, которые были инициированы внутри самой ИТ-организации, например, решает инциденты, обнаруженные автоматически или вручную ИТ-персоналом, или принимает Запросы на Обслуживание от других подразделений ИТ-организации.

Данная глава отличается от других глав книги, поскольку в ней основное внимание уделяется функции, организационной единице или подразделению, а не процессам, как в других главах. Эта тема включена в книгу, потому что Служба Service Desk играет важнейшую роль в ИТ Сервис-менеджменте. Для обозначения более широкого спектра деятельности в книге используется понятие Service Desk, вместо употребляемого долгое время термина Help Desk. Служба Help Desk обычно участвовала только в Процессе Управления Инцидентами, в то время как Служба Service Desk охватывает более широкий спектр деятельности ИТ.

Служба Service Desk выполняет действия в рамках ряда базовых процессов ITIL, а именно:

- В первую очередь это **Процесс Управления Инцидентами**, т. к. большая часть инцидентов принимается (регистрируется) Службой Service Desk и многие обращения в службу имеют отношение именно к инцидентам. В функции Службы Service Desk входит координация действий организаций поставщиков, участвующих в обработке инцидентов.
- На Службу Service Desk могут быть возложены обязанности по установке оборудования и программного обеспечения, и соответственно, она может играть определенную роль в **Процессах Управления Релизами или Изменениями**.
- Если при регистрации инцидента Служба Service Desk проверяет информацию о пользователе и детали Конфигурации его ИТ-ресурсов, то в этом случае Служба участвует в **Процессе Управления Конфигурациями**.

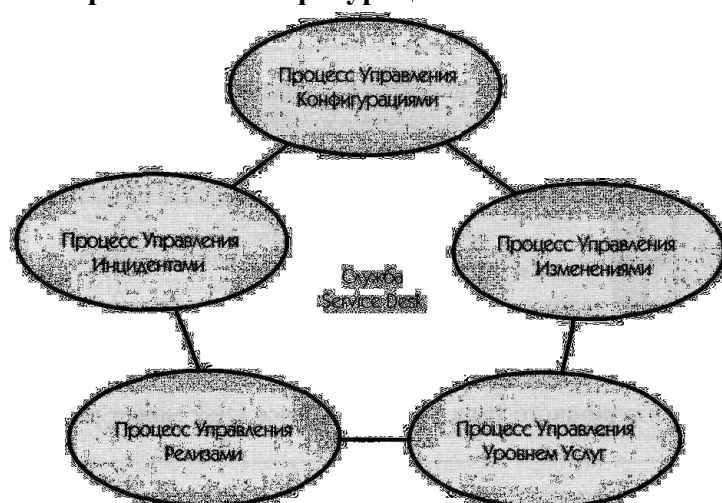


Рис. 9.1. Процессы, в которых участвует Служба Service Desk

- Служба Service Desk может выполнять Стандартные Запросы, такие как подключение к LAN и перемещение рабочих станций, в этом случае она участвует в оценке и проведении изменений и, следовательно, в **Процессе Управления Изменениями**.

- Служба Service Desk информирует пользователей о поддерживаемых ею продуктах и услугах. Если Служба не имеет полномочий на выполнение какого-либо Запроса, ей следует вежливо сообщить пользователю об этом и известить **Процесс Управления Уровнем Услуг** о поступившем Запросе.

Служба Service Desk также может выполнять действия, связанные с рядом других процессов ИТIL, например, с Процессом Управления Инфраструктурой (Операционная деятельность). Служба поддерживает взаимодействие с заказчиками, предоставляя информацию о поддерживаемых сервисах. Кроме этого Служба Service Desk является точкой ежедневных контактов с пользователями и средством мониторинга степени их удовлетворенности.

9.2. Цель

Основной целью Службы Service Desk является поддержка услуг, предоставляемых ИТ-организацией на основе достигнутых с заказчиком договоренностей, путем выполнения ряда действий по поддержке (из разных процессов).

Являясь точкой контакта с пользователями, Служба Service Desk позволяет уменьшить нагрузку на другие ИТ-подразделения путем «перехвата» не относящихся к делу обращений и вопросов, на которые легко ответить. Служба Service Desk действует как фильтр, который пропускает звонки на вторую и третью линии поддержки, только когда это действительно необходимо. Как единая точка контактов, Service Desk всегда действует профессионально при общении с пользователями и оберегает их от бесконечных поисков решения.

9.3. Структура

9.3.1. Доступность¹

Одной из основных задач Службы Service Desk является обеспечение доступа пользователей к ИТ-организации. Следует поощрять пользователей обращаться в Службу Service Desk, если у них есть вопросы или им нужна поддержка. Возможно осуществлять мониторинг способа обращений с помощью отчетов, предоставляемых телефонной станцией PABX.

Для создания благоприятного впечатления Служба Service Desk в своей работе с заказчиками должна действовать квалифицировано и быть последовательной. Этому могут способствовать специально разработанные процедуры взаимодействия и стандартные анкеты (опросники)² с вариантами стандартных ответов.

Для обеспечения доступа в Службу Service Desk могут использоваться различные технические средства, хотя телефон и электронная почта являются самыми распространенными. Также возможно использование голосовой почты, факса, интернета и автоматически генерируемых текстовых сообщений (например, для мобильных телефонов и пейджеров).

9.3.2. Поддержка бизнеса

Звонки можно разделить на несколько групп: звонки, связанные с инцидентами в технической инфраструктуре; звонки, связанные с инцидентами и вопросами по использованию приложений; звонки с вопросами о статусе услуг (ходе работы над инцидентами), Запросы на Стандартные Изменения и другие Запросы. В зависимости от организационного типа, Служба Service Desk может рассматривать либо все обращения или только те обращения, которые связаны с техническими проблемами и запросами, а поддержку приложений оставить заказчику. В последнем случае подразделение заказчика, где используется приложение, контактирует со Службой поддержки бизнес-операций³. Данная Служба будет отвечать на вопросы пользователей

¹ Accessibility.

² ScriDts.

³ Business operations support desk.

по приложениям, а технические вопросы направлять в Службу Service Desk ИТ-организации. При такой организации работы Служба Service Desk не будет перегружена вопросами, связанными с использованием приложений.

9.3.3. Варианты организации

Существует несколько вариантов организации Служб Service Desk. Наиболее распространенными являются следующие:

- **Централизованная Служба Service Desk** как единая точка контакта для всех пользователей, возможно с отдельной Службой Service Desk, расположенной ближе к пользователям бизнес-приложений (Service Desk с разделением функций).
- **Локальные (распределенные) Службы Service Desk**, расположенные на нескольких объектах. Обычно такое деление Службы Service Desk усложняет управление.
- **Виртуальная Служба Service Desk**, когда ее географическое расположение не имеет значения в связи с использованием коммуникационных и Интернет-технологий.

Централизованная Служба Service Desk

На рис. 9.2 показана структура Централизованной Службы Service Desk с разделением функций. Если ИТ-организация несет ответственность и за предоставление услуг, и за поддержку информационных систем, то лучше всего, чтобы Служба Service Desk была для пользователей единой точкой контактов. В этом случае Service Desk отвечает за прием, регистрацию, мониторинг хода обработки и эскалацию звонков. Функция поддержки бизнес-операций может являться частью функций Службы Service Desk или же за это может отвечать отдельная группа поддержки, контролируемая Службой Service Desk. Для такой организации работы требуется общая система регистрации инцидентов. Если ИТ-организация не несет ответственности за поддержку бизнес-операций, тогда служба поддержки бизнес-операций будет действовать от лица пользователей в тех случаях, когда требуется поддержка со стороны поставщика ИТ-услуг.

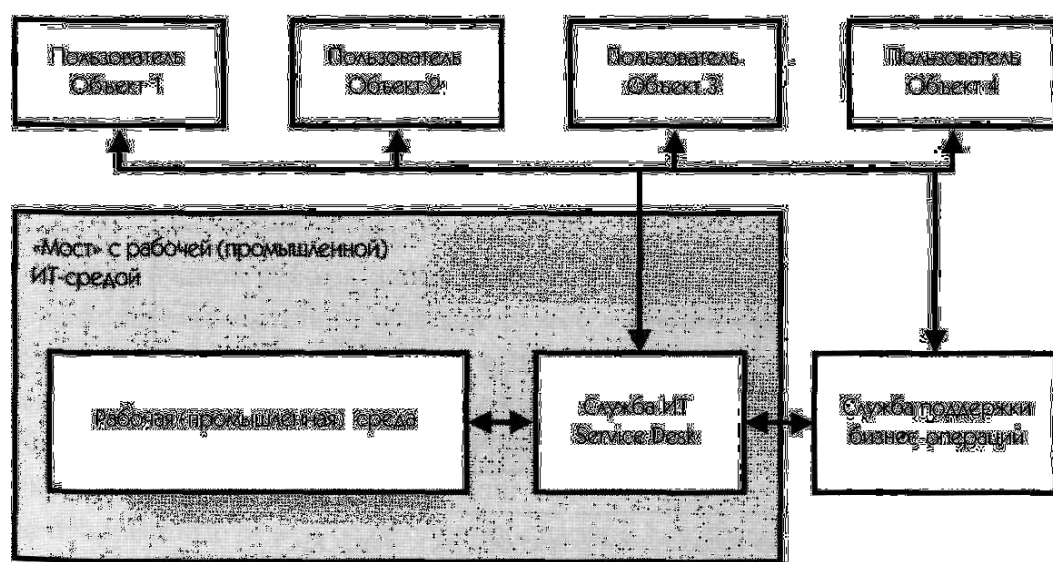


Рис 9.2. Служба Service Desk с разделением функций

Такой подход может сочетаться с организацией «моста» с операционной средой¹ (т.е. точкой концентрации руководства операционной деятельностью, которой может выступать, например, Служба Service Desk в сочетании с отделом эксплуатации²). Это может быть целесообразно для обеспечения взаимодействия между Службой Service Desk и руководством

¹ Operations bridge.

² Под отделом эксплуатации (операционным отделом) понимается группа обеспечения операционной деятельности – Operations department. – Прим. ред.

операционной деятельностью¹, включая Управление Сетями, Серверами и т.д. Такое взаимодействие Службы Service Desk с функциональными подразделениями ИТ обеспечивает быстрое реагирование в тех случаях, когда Служба Service Desk не может сразу же устранить ошибки. В идеале эти подразделения должны размещаться близко друг к другу.

Распределенная Служба Service Desk

Распределенная служба размещается в разных зданиях или даже в разных городах и регионах. На рис. 9.3 представлен пример распределенной Службы Service Desk. При использовании такой структуры целесообразно выбрать один из предлагаемых ниже вариантов:

- **Центральная точка контактов**, где звонки принимаются и далее маршрутизируются в локальные службы поддержки. Центральная Служба Service Desk является для пользователей начальной точкой контактов, где регистрируются инциденты. Современное программное обеспечение маршрутизации звонков способствует повышению эффективности работы Службы Service Desk в разрешении инцидентов.

- **Локальные точки контактов** с центральной Службой Service Desk предназначены для отслеживания и мониторинга инцидентов. Данный подход часто используется в тех случаях, когда у локальной организации свой язык и корпоративная культура, а также когда у организации достаточно много специфических приложений собственной разработки для каждого направления бизнеса. Например, у компании в химической отрасли может быть более трехсот категорий собственных приложений, а общее количество приложений – около тысячи. В такой ситуации единственным практическим решением является распределение функции Службы Service Desk различными направлениями бизнеса, т.к. для решения инцидентов требуются специфические знания в конкретной области. Локальная ответственность за затраты на поддержку может служить дополнительным мотивирующим фактором в такой структуре.

- **Центр обработки звонков (Call Center)**. Этот вариант становится все более популярным, и его часто используют провайдеры и поставщики услуг. По центральному номеру телефона, обычно бесплатному, можно получить доступ к главному меню, из которого пользователь выбирает пункт, по которому требуется помощь, например, электронная почта или офисные приложения. Звонок затем направляется к специалисту соответствующей группы поддержки. Эти группы могут находиться в разных местах, но пользователь об этом может даже не подозревать.

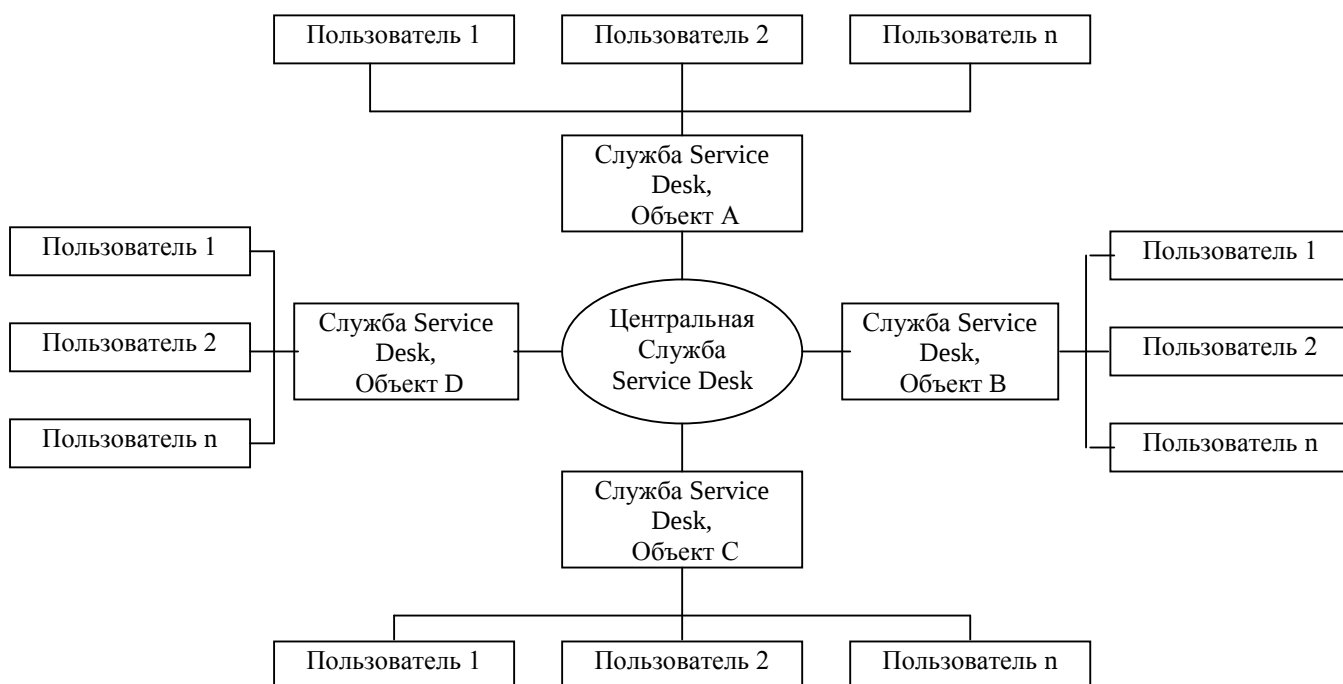


Рис. 9.3. Распределенная служба Service Desk с централизованным управлением (источник: OGC)

¹ Production, Operations.

Виртуальная Служба Service Desk

Виртуальная служба Service Desk является современной специализированной версией распределенной службы. Она состоит из нескольких локальных Служб Service Desk, которые образуют единую (виртуальную) службу, поскольку современные телекоммуникационные и Интернет - технологии делают месторасположение несущественным фактором. В таком случае Служба Service Desk и группы поддержки могут располагаться где угодно. Имея локальные службы в разных временных зонах, такая служба обеспечивает круглосуточную поддержку пользователей (концепция «следующая за солнцем»). Недостатком такой организации является трудность предоставления поддержки на местах.

В последнее время мы видим возможности самостоятельного получения помощи пользователями (самообслуживания-self-help) как форму «автоматизированной» функциональности Службы Service Desk.

Например, возможность самообслуживания посредством Web-доступа к базе знаний (поиск известных ошибок) и записям инцидентов (проверка статуса и т.д.), способствует сокращению расходов и созданию сообщества пользователей.

1. Персонал Службы Service Desk

Требования к персоналу Службы Service Desk определяются ее миссией и структурой. Ниже даются возможные варианты основных способов построения и требования к персоналу, вытекающие из поставленных задач:

- **Центр обработки звонков (Call Center):** производит только запись/регистрацию звонков и не предоставляет какой-либо поддержки. Обращения перенаправляются к специалистам соответствующих подразделений для обработки. В некоторых случаях можно автоматизировать запись и маршрутизацию обращений с помощью голосовых меню.

- **Неквалифицированная Служба Service Desk или Служба регистрации звонков:** все звонки регистрируются, описываются в общих чертах и затем сразу маршрутизируются. Служба Service Desk в основном выполняет диспетчерские функции, и для обработки поступающих звонков ей необходимы стандартные процедуры работы и сценарии обработки обращений (опросники). Для обеспечения успешной работы необходимо наличие опытного руководителя и хорошей дисциплины. Преимуществом данного подхода является стандартизация приема и регистрации инцидентов, а недостатком - более длительное время реакции и более низкая степень решения инцидентов при первом обращении по сравнению с квалифицированной Службой Service Desk.

- **Квалифицированная Служба Service Desk:** этот тип Службы Service Desk предполагает наличие высокого уровня профессиональной подготовки и большого опыта у персонала. Используя документированные решения, сотрудники данной службы могут решать большую часть всех поступающих инцидентов, хотя некоторые из них все же перенаправляются в группы поддержки. Степень решения инцидентов при первом обращении у такой службы обычно бывает выше, чем у неквалифицированной Службы Service Desk.

- **Экспертная Служба Service Desk:** персонал данной службы знает всю ИТ-инфраструктуру и располагает экспертными знаниями, позволяющими решать инциденты самостоятельно.

9.3.5. Технологии для работы Службы Service Desk

Существует много технических вариантов организации Службы Service Desk. Помимо рассмотрения эффективных инструментальных средств ИТ Сервис-менеджмента, должны быть также рассмотрены следующие аспекты:

- интеграция инструментальных средств сервис-менеджмента с системами Управления ИТ инфраструктурой;
- коммуникационные технологии, такие как Computer Telephone Integration (CTI) или Voice Over Internet Protocol (VOIP);
- системы интерактивного речевого меню (Interactive Voice Response — IVR);

- электронная почта (E-Mail);
- факс-серверы (факс через электронную почту или Интернет);
- инструментальные средства перенаправления звонков на пейджеры, мобильные телефоны и портативные компьютеры;
- инструментальные средства поиска и диагностики неисправностей (базы знаний, системы принятия решения по ситуации);
- автоматизированные инструментальные средства Управления Сетями и Системами;
- Инtranет и Интернет-порталы для самостоятельного доступа пользователей.

9.4. Виды деятельности

9.4.1. Ответы на обращения

Обращение (звонок) — это контакт пользователя со Службой Service Desk. Все обращения пользователей должны регистрироваться для облегчения дальнейшей обработки, мониторинга хода обработки и предоставления метрик, необходимых для контроля над процессом.

Существует две категории обращений:

- **Инциденты:** по существу, это все обращения, за исключением тех, что связаны со стандартными изменениями:

- Сообщения об ошибках: реальные сбои в инфраструктуре и жалобы на услуги.

- Запросы на Обслуживание¹: в библиотеке ITIL Запросы на Обслуживание классифицируются как инциденты, но они не предполагают наличия сбоя в инфраструктуре. Эти Запросы также не попадают в сферу действия Процесса Управления Изменениями. Примером такого Запроса могут послужить вопросы типа «Как мне сделать?», Запросы на Информацию, например, Запросы о Статусах Систем, Запросы на Документацию или получение рекомендации, Запросы на Смену паролей, Запросы на Запуск Пакетных Заданий, восстановление файлов или получение информации из базы данных, Запросы на расходные материалы (включая замену мыши, клавиатуры и т. д., если они не являются Конфигурационными Единицами), на предоставление документации, например, руководства пользователя и т. д.

- **Изменения:** в большинстве случаев это стандартные Запросы на Изменения (RFC). В некоторых случаях Служба Service Desk также отвечает за перемещение оборудования. Стандартное изменение на практике представляет собой типовое (рутинное) изменение инфраструктуры, которое выполняется по установившейся известной схеме (процедуре) и является согласованным (одобренным) решением в ответ на какие-либо требования или группу требований. Примерами стандартного изменения может служить апгрейд PC для использования специального программного обеспечения; настройка PC, установка стандартного набора программного обеспечения и подключение к сети новых сотрудников; простые стандартизированные настройки и заказ стандартных рабочих станций, периферийных устройств и локальных приложений. Основное различие между Запросом на Обслуживание и стандартным изменением состоит в том, что первый регистрируется как инцидент, который не требует изменения в ИТ-инфраструктуре, в то время как второй регистрируется как изменение и требует проведения изменения в ИТ-инфраструктуре.

Примечание. Согласно библиотеке ITIL оба типа обращений (сообщения об ошибках и Запросы на Обслуживание) рассматриваются как «инциденты», т. к. они обрабатываются по достаточно близким правилам. С другой стороны, ITIL допускает использование отдельных процедур для обработки Запросов на Обслуживание, которые отделены от Процесса Управления Инцидентами.

¹ Accounts.

9.4.2. Предоставление информации

Служба Service Desk должна служить основным источником информации для пользователей. Способ предоставления информации может быть пассивным (например, через электронную доску объявлений) или активным (электронная почта, Web-доступ к автоматизированной системе Службы Service Desk, экранные формы и др.). Необходимо сделать все возможное для информирования пользователей о текущих или ожидаемых ошибках, и лучше делать это до того, как эти ошибки затронут пользователя. Служба Service Desk также должна предоставлять информацию о новых и имеющихся услугах, условиях Соглашений об Уровне Услуг (SLA), а также о процедурах заказа услуг и ценах.

9.4.3. Взаимодействие с поставщиками

Служба Service Desk часто отвечает за взаимодействие с обслуживаемыми организациями и внешними поставщиками. Это касается ремонта и замены принтеров, рабочих станций и в некоторых случаях телекоммуникационного оборудования. Такой тип поддержки может быть использован при обработке инцидентов, в своем первоначальном значении — сбоев, а также инцидентов в смысле Запросов на Обслуживание и Изменений.

9.4.4. Операционные задачи

Примерами таких задач могут быть создание резервных копий и восстановление данных из архива, подключение к локальной сети, Управление Дискковой Памятью на локальных серверах, создание учетных записей¹, авторизация и смена паролей.

9.4.5. Мониторинг инфраструктуры

Служба Service Desk может иметь в своем распоряжении инструментальные средства, помогающие определению степени воздействия сбоев на работу критически важных систем, таких как маршрутизаторы, серверы, шлюзы, приложения и базы данных. Часто эти средства автоматически обнаруживают сам сбой или угрозу его возникновения и передают информацию в Процесс Управления Инцидентами. Службе Service Desk необязательно применять эти средства, т. к. обнаружение сбоев является главной задачей операционных подразделений² ИТ, которые и передают эту информацию Службе Service Desk.

9.5. Эффективность³

Удовлетворенность заказчика или пользователя является основным показателем эффективности работы Службы Service Desk. Примерами Ключевых параметров эффективности (KPI) могут быть:

- скорость ответа на телефонные звонки (например, на 90% телефонных звонков отвечают в течение X секунд);
- скорость перенаправления звонков на вторую линию поддержки в течение X минут (если звонок нельзя разрешить на уровне Service Desk).
- восстановление сервиса в течение допустимого времени и в соответствии с условиями Соглашения об Уровне Услуг (SLA);
- своевременное информирование пользователей о текущих и будущих изменениях и ошибках.

Некоторые показатели эффективности можно определить только на основе результатов опроса заказчиков, например такие как:

- Насколько вежливо специалисты Service Desk общаются по телефону?

¹ Accounts

² Operations.

³ Effectiveness

- Предоставляются ли пользователям хорошие рекомендации по способу предотвращения инцидентов?

9.5.1. Отчеты руководству

Служба Service Desk должна регулярно (например, раз в полгода) проверять, насколько ее работа отвечает заданным стандартам. Примерами метрик являются:

- процент инцидентов, которые могут решаться на Уровне Service Desk без перенаправления на другие уровни поддержки (например, на вторую или третью линии поддержки или к поставщику);
- количество обработанных звонков на одно рабочее место/пользователя и общее количество звонков, обработанных Службой Service Desk;
- среднее время решения инцидентов (по степени воздействия) или время, необходимое для выполнения Запроса на Обслуживание. Следует указывать как непосредственное время на выполнение, так и общее время от открытия до закрытия инцидента;
- отчеты телефонной станции (PABX) о среднем времени ответа на телефонный звонок, количестве звонков, прерванных пользователями, средней продолжительности звонков и соответствующих метрик на каждого специалиста Службы Service Desk.

Для этих метрик могут быть определены стандарты, по которым возможно отслеживание улучшения или ухудшения в предоставлении услуг. Эффективность Службы Service Desk также может быть измерена путем проведения регулярных опросов и анкетирования пользователей в компании.

9.5.2. Критические факторы успеха

Если в Службу Service Desk невозможно дозвониться, тогда пользователи перестанут обращаться и постараются исправить ошибки самостоятельно или найти кого-либо в своей организации, кто помог бы им решить вопросы. Поэтому до публичного анонсирования необходимо вывести Службу Service Desk на требуемый уровень.

Если пользователи пытаются установить контакты напрямую со специалистами, их следует направлять в Службу Service Desk.

Для того, чтобы поддержка, оказываемая Службой Service Desk была сфокусированной, следует тщательно прорабатывать Каталог услуг, Соглашения об Уровне Услуг (SLA) и Операционные Соглашения об Уровне Услуг (OLAs).

Глава 10

Управление Уровнем Сервиса (Услуг)

10.1. Введение

Управление Уровнем Сервиса (Услуг) — это процесс, в рамках которого происходят переговоры по вопросам предоставления услуг, производится определение, измерение (оценка), управление и улучшение качества ИТ-услуг при соблюдении приемлемого Уровня Затрат. Все эти задачи должны решаться в условиях быстро меняющихся потребностей бизнеса и быстро развивающихся технологий. Процесс Управления Уровнем Сервиса помогает найти нужный баланс между предложением и спросом на услуги требуемого Уровня Качества, их легкостью в использовании и стоимостью. И поставщик, и заказчик должны четко осознавать, что услуги не только поставляются, но и используются. Это понимание реализуется в разработке, согласовании и выполнении Соглашений об Уровне Услуг¹ (SLA), Операционных Соглашений об Уровне Услуг² (OLA), Внешних Договоров³ (UC) и Плана Обеспечения Качества Услуг⁴⁴ (SQP).

10.1.1. Основные понятия

Поставщики и заказчики ИТ-услуг

Теоретически, любой, кто получает ИТ-услуги, является заказчиком. В большинстве случаев ИТ-организация является поставщиком, но поскольку обычно она тоже получает ИТ-услуги, то одновременно выступает и как заказчик ИТ-сервисов у Сервис-провайдеров. Все это создает достаточно сложную сеть взаимоотношений. Например, подразделение разработки программного обеспечения может запросить у отдела центрального процессинга услуги в режиме онлайн, и одновременно это же подразделение выполняет сопровождение ПО для обеспечения непрерывности запрашиваемых им же услуг. Теоретически Управление Уровнем Сервиса является линейным процессом, нацеленным на определение услуг и заключение соглашений, таких как Внешние Договоры (UC) с внешними поставщиками, Операционные Соглашения об Уровне Услуг (OLA) с внутренними поставщиками или Соглашения об Уровне Услуг (SLA) с заказчиками. Однако в данном вопросе требуется гибкий подход, так как различие между заказчиком и поставщиком ИТ-сервисов не всегда бывает четким. В контексте Процесса Управления Уровнем Услуг мы используем следующие определения заказчика и поставщика:

- **Заказчик** — это представитель организации, у которого есть полномочия на заключение соглашений от лица организации на получение ИТ-услуг. Поэтому заказчик и конечный пользователь услуг — не одно и то же.
- **Поставщик** — это представитель организации, у которого есть полномочия на заключение соглашений о предоставлении ИТ-услуг.

Требования к Уровню Услуг (Service Level Requirements — SLR)

Требования к Уровню Услуг представляют собой детальное описание потребностей заказчика, они используются при разработке, модификации и инициировании услуг. Такие требования можно использовать в качестве прототипа (кальки) для разработки услуги и соответствующего ей Соглашения об Уровне Сервиса (SLA), а также как проектное задание (design assignment).

Таблицы спецификации сервисов (Service Specification Sheets — Spec Sheets)

Таблицы спецификаций используются для описания зависимости отношений между функциональностью (согласованной с заказчиком и поэтому определяемой извне, с точки зрения

¹ Service Level Agreements - SLA.

² Operational Level Agreements — OLA.

³ Underpinning Contracts - UC.

⁴ Service Quality Plan - SQP.

поставщика) и технологией (используемой в организации и потому управляемой изнутри) и содержат детальную спецификацию услуги. Таблицы помогают преобразовать Требования к Уровню Сервисов (внешние спецификации) в технические определения, необходимые для предоставления этой услуги (внутренние спецификации). Кроме того, они описывают связи между соглашениями SLA, OLA и UC. Таблицы спецификаций являются важным инструментом мониторинга соответствия внутренних спецификаций внешним.

Каталог услуг (Service Catalog)

Разрабатывая Каталог услуг, ИТ-организация создает о себе представление как о поставщике ИТ-услуг, а не просто как о технологической организации, выполняющей внедрение и сопровождение технических средств и ПО. Каталог содержит подробное описание действующих услуг на понятном заказчику языке, а также описание Уровней Сервисов, которые организация может предложить своим заказчикам. В этом плане Каталог является важным коммуникативным инструментом. Каталог услуг может помочь в формировании ожиданий пользователя и тем самым облегчить процесс согласования целей и задач заказчика и поставщика услуг. Каталог создается на основе внешних спецификаций и поэтому должен быть написан понятным заказчику языком, а не языком технических спецификаций.

Соглашение об Уровне Услуг (Service Level Agreement — SLA)

Соглашение об Уровне Услуг представляет собой соглашение между ИТ-организацией и заказчиком, в котором подробно оговорены предоставляемые услуги. Данное соглашение описывает услуги в нетехнических терминах, на уровне понимания заказчика, и в течение срока действия соглашения оно является стандартом для оценки и корректировки ИТ-сервисов. Соглашение обычно имеет иерархическую структуру, например, услуги общего характера, такие как сетевые услуги и услуги службы Service Desk, определяются для всей организации и утверждаются руководством. Услуги более конкретного характера, предназначенные для бизнес-деятельности, согласуются на более низком уровне, например, с руководством бизнес-подразделения, владельцем бюджета или представителем заказчика.

Программа улучшения сервиса (Service Improvement Program — SIP)

Данная программа часто реализуется как проект, в рамках которого определяются виды деятельности по улучшению качества ИТ-сервисов, этапы и контрольные точки в данной работе.

План обеспечения качества услуг (Service Quality Plan — SQP)

План обеспечения качества сервиса является важным документом, так как в нем содержится вся информация, необходимая для управления ИТ-организацией. В нем определены параметры процессов сервис-менеджмента и операционного управления. Если Соглашение SLA определяет *что* мы будем предоставлять, то План SQP определяет *как* мы будем это предоставлять. В плане обеспечения качества определены цели улучшения для каждого процесса в форме Показателей качества (Performance indicators). Например, для Процесса Управления Инцидентами план определяет время разрешения для инцидентов в зависимости от различной степени воздействия, а для Процесса Управления Изменениями — время цикла и затраты на стандартные изменения, например, такие как перемещение сотрудников. Для всех процессов определяются виды отчетов и сроки их предоставления. Показатели качества разрабатываются на основе Требований к Уровню Услуг и заносятся в Таблицы спецификаций. Если в предоставлении услуг участвуют внешние поставщики, например, когда к службе Service Desk или к обслуживанию персональных компьютеров привлекаются внешние ресурсы, тогда Показатели качества определяются во Внешних Договорах.

Операционное Соглашение об Уровне Услуг (Operational Level Agreement — OLA)

Это соглашение с внутренним ИТ-подразделением, в котором конкретизируются договоренности о предоставлении определенных элементов сервисов, например, доступности сети или доступности серверов печати. Например, если соглашение SLA содержит временные показатели в разрешении инцидентов с высоким приоритетом, то Операционное Соглашение об Уровне Услуг (OLA) должно определять цели для каждого элемента цепочки поддержки (параметры для службы Service Desk — время ответа на звонки, эскалация инцидентов и т. д., параметры для Службы поддержки сети — сроки расследования и устранения сетевых ошибок и т. д.). Операционные Соглашения об Уровне Услуг помогают ИТ-организации в общем процессе предоставления услуг.

Внешний Договор (Underpinning contract — UC)

Это договор с внешним поставщиком, который определяет договоренности по предоставлению конкретных услуг, например, поддержку рабочих станций или аренду линии связи. Действие такого договора аналогично внешней реализации соглашения OLA. Во многих организациях ИТ-услуги предоставляет внутреннее ИТ-подразделение. В этом случае соглашения SLA и OLA в большей степени представляют собой описание того, о чем договорились между собой внутренние подразделения, чем юридический документ. Однако договор с внешним поставщиком обычно оформляется в форме официального правового документа.

10.2. Цель процесса

Процесс Управления Уровнем Сервиса гарантирует постоянную поддержку и совершенствование требуемых заказчиком ИТ-услуг. Это достигается путем согласования Уровня Качества Услуг ИТ-организации, их мониторинга и предоставления отчетов, что способствует установлению эффективных взаимоотношений между ИТ-организацией и ее заказчиками.

Эффективный Процесс Управления Уровнем Сервиса способствует более успешному ведению бизнеса и ведет к большей удовлетворенности заказчика. Поскольку ИТ-организация будет лучше осведомлена о том, что ожидают от нее заказчики и что она может предоставить, у нее будет больше возможностей улучшить планирование услуг, составление бюджета и управление услугами.

Преимущества использования процесса

В целом, введение в практику Процесса Управления Уровнем Сервиса может дать следующие преимущества:

- ИТ-услуги разрабатываются в соответствии с Требованиями к Уровню Услуг и, следовательно, будут отвечать ожиданиям заказчика;
- качество услуг можно будет оценить/измерить, и, следовательно, им можно будет управлять и составлять отчеты;
- если ИТ-организация выставляет счета заказчику за пользование ИТ-услугами, то заказчик сможет сопоставить Уровень Качества услуг с предъявленной в счете стоимостью;
- поскольку ИТ-организация может создавать спецификации требуемых услуг и их компонентов, она получает возможность участвовать в управлении ресурсами и способствовать долговременному сокращению затрат;
- улучшаются отношения с заказчиками и повышается уровень удовлетворенности потребителей ИТ-услуг;
- и заказчик, и ИТ-организация знают о своих обязанностях и ролях, следовательно, будет меньше недопонимания и упущений.

10.3. Процесс

Управление Уровнем Сервиса — это процесс, который связывает поставщика ИТ-услуг и заказчика. Этот процесс имеет следующие задачи:

- интеграцию элементов, необходимых для предоставления ИТ-услуг;
- документирование услуг путем четкого описания их элементов в различных документах;
- описание предоставляемых заказчику услуг на понятном и удобном для заказчика языке;
- согласование ИТ-стратегии с потребностями бизнеса;
- контролируемое улучшение предоставления ИТ-услуг.

Управление Уровнем Сервиса играет центральную роль в процессах ИТ Сервис-менеджмента и тесно связано с Процессами Поддержки и Предоставления услуг. Данный процесс служит мостом между заказчиком и поставщиком ИТ-услуг, так как он дает возможность обсуждать бизнес-потребности заказчика без углубления в технические детали. Затем запросы заказчика ИТ-организация преобразует в технические спецификации и конкретные виды деятельности. Степень невовлеченности заказчика в технологические вопросы является показателем успешной работы процесса. Управление Уровнем Сервиса требует эффективного и продуктивного сотрудничества с заказчиком, так как уровни запрашиваемых услуг определяются при его участии. Если заказчик (бизнес) не знаком с предметом обсуждения, то начинать следует именно с этого. На рис. 10.1 представлена последовательность действий в рамках Процесса Управления Уровнем Сервисов. На ней показаны два компонента, составляющих процесс, которые во многом выполняются параллельно: первый, более высокого уровня, связан с выработкой договоренностей, второй, более низкого уровня, — с обеспечением выполнения достигнутых договоренностей.

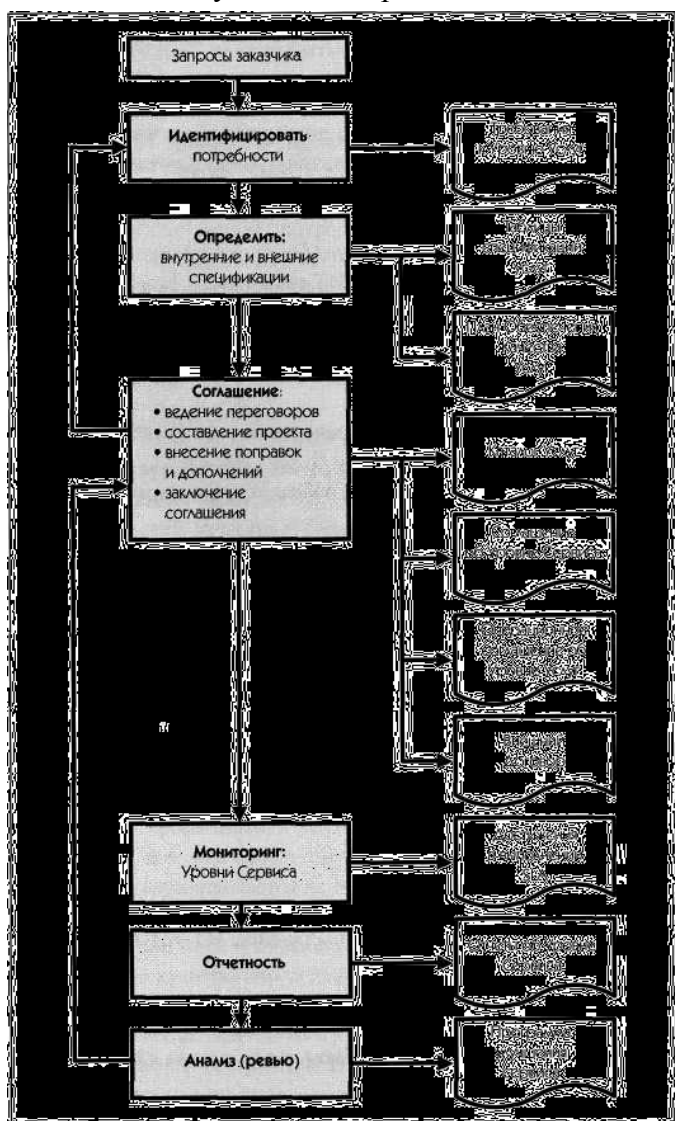


Рис. 10.1. Процесс Управления Уровнем Сервисов

В рамках Процесса Управления Уровнем Сервиса выполняются следующие виды деятельности:

- **Идентификация** — идентификация потребностей заказчика, управление взаимоотношениями и внутреннее продвижение¹ ИТ-организации. Понимание бизнес-процессов и потребностей заказчика.
- **Определение** — определение требуемых услуг в соответствии с потребностями и запросами заказчика. Услуги определяются в виде Требований к Уровню Услуг и Таблиц спецификаций услуг. Результатом выполнения этого вида работ является создание Плана обеспечения качества услуг.
- **Окончательное оформление соглашения** — заключительный этап работы над соглашением, т. е. обсуждение с заказчиком требуемого Уровня Сервисов и связанных с этим затрат, закрепление достигнутых договоренностей в Соглашении об Уровне Сервиса (SLA). Подкрепление соглашения SLA Операционными Соглашениями об Уровне Услуг (OLA) и Внешними Договорами (UC). Составление или обновление Каталога Услуг с указанием в нем доступных для заказчиков услуг.
- **Мониторинг** — мониторинг Уровней Сервисов.
- **Отчетность** — составление Отчетов об Уровне Сервисов. Регулярное предоставление отчетов заказчику и ИТ-организации о реальных текущих Уровнях Предоставления Услуг в сравнении с общим достигнутым Уровнем (Service Level Achievement).
- **Анализ (пересмотр)** — совместный с заказчиком анализ сервисов с целью определения направлений его улучшения. Возможно инициирование Программы улучшения сервиса, если это необходимо. Деятельность включает в себя частые контакты с заказчиком и обмен мнениями о предоставляемых услугах. Результатом такого вида деятельности может стать новое или пересмотренное Соглашение об Уровнях Сервиса.

Для эффективной работы Процесса Управления Уровнем Сервиса требуется наличие других Процессов Поддержки и Предоставления услуг. Все эти процессы в определенной степени содействуют успешному Управлению Уровнем Сервисов. При определении услуги и соответствующего Уровня предоставления необходимо учитывать степень развития Процессов Поддержки Услуг. Ниже дается общее описание взаимоотношений Управления Уровнем Услуг с другими процессами.

Взаимоотношения со Службой Service Desk

Хотя Служба Service Desk является функцией (функциональным подразделением), а не процессом, ее взаимосвязь с Процессом Управления Уровнем Сервиса является особенно важной. Служба Service Desk является начальной точкой контактов для пользователей, и ее цель в случае возникновения сбоя — восстановить согласованный Уровень Предоставления Услуг как можно скорее посредством Процесса Управления Инцидентами. Поскольку данная служба напрямую контактирует с пользователями, она может предоставить ценную информацию об их восприятии Уровня Сервисов (степени удовлетворенности). Обычно существует сильная зависимость между степенью удовлетворенности пользователя и заказчика. Служба Service Desk также играет важную роль в определении времени реагирования и времени разрешения при возникновении сбоя в предоставлении сервисов.

Взаимоотношения с Процессом Управления Доступностью

Процесс Управления доступностью отвечает за реализацию и оптимизацию доступности услуг. Управление Уровнем Сервиса предоставляет Процессу Управления доступностью входную информацию о требуемом Уровне Доступности ИТ-услуг, и этот процесс, в свою очередь, дает Управлению Уровнем Услуг информацию о реально существующем Уровне Доступности ИТ-сервисов.

¹ Promotion.

Взаимоотношения с Процессом Управления Мощностями

Задача Процесса Управления Мощностями — управлять мощностями и пропускной способностью ИТ-инфраструктуры. Для этого создается План мощностей (Capacity Plan), который детализирует текущее использование инфраструктуры и прогнозирует ее будущее использование. Содействие

Процесса Управления Мощностями состоит в том, что он предоставляет Управлению Уровнем Сервиса информацию о степени воздействия новой услуги или расширения уже имеющейся услуги на общий Уровень ИТ-мощностей, а также о том, находится ли потребление конкретной услуги в заранее согласованных пределах.

Управление Уровнем Услуг предоставляет Процессу Управления Мощностями информацию об ожидаемом текущем и будущем Уровне Использования Услуги, которое уже согласовано или будет согласовано с заказчиком.

Взаимоотношения с Процессами Управления Инцидентами и Проблемами

Процессы Управления Инцидентами и Проблемами являются хорошими индикаторами эффективной реализации соглашений SLA. В частности, Процесс Управления Инцидентами играет особенно важную роль в скорейшем восстановлении услуг после возникновения сбоя.

Процесс Управления Проблемами помогает оптимизировать стабильность услуг благодаря постоянно предпринимаемым им мерам по предотвращению возникновения ошибок.

Наличие механизмов разрешения инцидентов и проблем является необходимым условием для предоставления высококачественных услуг. Процесс Управления Уровнем Сервиса использует информацию из этих процессов при составлении своих отчетов заказчику.

Взаимоотношения с Процессом Управления Изменениями

В соглашении SLA могут быть определены изменения, которые запрашивает организация заказчика, и соглашения, которые будут регулировать эти изменения (кому изменения адресованы, какое время цикла, затраты, способы информирования организации и т. д.). Изменение может повлиять на уже согласованные Уровни Сервисов.

Взаимоотношения с Процессом Управления Релизами

Многие ИТ-услуги состоят в предоставлении аппаратного обеспечения вместе со сделанным на заказ или готовым программным обеспечением. Процесс Управления Релизами ведет мониторинг соглашений, заключенных в рамках Процесса Управления Уровнем Сервисов, о предоставлении аппаратного и программного обеспечения. Процесс Управления Уровнем Сервиса подготавливает отчеты о качестве ИТ-сервисов на основе информации, получаемой из отчетов Процесса Управления Релизами.

Взаимоотношения с Процессом Управления Непрерывностью ИТ-услуг

Процесс Управления Непрерывностью ИТ-услуг отвечает за быстрое восстановление ИТ-сервисов в случае катастрофы, а также он ведет мониторинг действий и процедур, необходимых для осуществления этого восстановления. Соглашения с заказчиком по данным вопросам заключаются в рамках Процесса Управления Уровнем Сервисов. Предпринимаемые в случае бедствия меры и связанные с ними затраты затем входят составной частью в Соглашение об Уровне Сервиса. Также может быть достигнута договоренность, что в случае чрезвычайных обстоятельств некоторые ИТ-сервисы не будут использоваться или будут временно сокращены.

Изменения в услуге и связанном с ней соглашении SLA могут потребовать модификации уже разработанных мер и процедур по обеспечению непрерывности услуг.

Взаимоотношения с Процессом Управления Безопасностью

Для эффективно действующего Процесса Управления Уровнем Сервиса большое значение могут иметь меры безопасности, связанные с ИТ-сервисом. Как у ИТ-организации, так и у заказчика могут быть определенные требования к безопасности. Соответствующие договоренности определяются в рамках Соглашения об Уровне Сервиса. Управление безопасностью гарантирует, что принимаются согласованные меры безопасности, ведется их мониторинг и составляются отчеты для Процесса Управления Уровнем Сервисов.

Взаимоотношения с Процессом Управления Конфигурациями

Процесс Управления Конфигурациями отвечает за ввод детальной информации о компонентах услуг (Конфигурационных Единицах) и документации (Соглашений об Уровне Сервиса — SLA) в Конфигурационную Базу Данных (CMDB) и предоставление информации из этой базы. Поэтому создание или модификация услуги или соглашения влечет за собой изменения в CMDB. Служба Service Desk использует Конфигурационную Базу Данных для определения степени воздействия сбоев на услуги и для получения информации из соглашений SLA о времени реагирования и времени разрешения сбоев. Информация из CMDB также используется при составлении отчетов о качестве Конфигурационных Единиц, что позволяет Процессу Управления Уровнем Сервиса подготавливать отчеты о качестве предоставляемых услуг.

Взаимоотношения с Процессом Управления Финансами ИТ

Если ИТ-организация выставляет заказчику счет за предоставленные услуги, то этот вопрос также должен быть отражен в SLA. Это могут быть одноразовые платежи или платежи за специальные или дополнительные услуги. Управление финансами предоставляет Процессу Управления Уровнем Сервиса информацию о затратах на предоставление услуг, а также информацию о методах и уровнях оплаты, необходимых для покрытия затрат на предоставление услуг.

10.4. Виды деятельности

Ниже дается подробное описание этапов процесса, включая последовательность действий и виды работ.

10.4.1. Идентификация

По мере усиления зависимости бизнеса от ИТ-сервисов возрастает спрос на высококачественные ИТ-услуги. Приемлемость качества услуги определяется ожиданиями заказчика, постоянным управлением этими ожиданиями, стабильностью услуги и приемлемостью Уровня Расходов. Поэтому самый лучший способ обеспечить соответствующий Уровень Качества — обсуждение этого вопроса с самим заказчиком.

Опыт показывает, что часто заказчики сами не могут четко определить свои ожидания, они просто предполагают, что им будут предоставлены некоторые услуги без каких-либо определенных договоренностей. Такое восприятие заказчиком процесса предоставления услуг часто приводит к серьезному недопониманию. И это еще раз подтверждает, насколько необходимо Руководителю Процесса Управления Уровнем Сервиса хорошо знать своих заказчиков, чтобы помочь разобраться, какие Услуги и на каком Уровне им действительно необходимы и с каким Уровнем Затрат.

Требования заказчиков должны быть представлены в поддающихся измерению значениях, с тем чтобы можно было их использовать при разработке и мониторинге ИТ-услуг. Если метрики не согласованы с заказчиком, то нельзя будет проверить, насколько услуги соответствуют достигнутым договоренностям. Процесс Управления Уровнем Сервиса играет ключевую роль в понимании и определении пожеланий заказчика.

Первым шагом к заключению Соглашения о предоставляемых в настоящий момент или в будущем ИТ-услугах должны стать идентификация и определение потребностей заказчика в виде Требований к Уровню Услуг (Service Level Requirements — SLR). Помимо выполнения этого вида деятельности в самом начале данного процесса, рекомендуется делать это регулярно по запросам заказчика или по инициативе самой ИТ-организации и охватывать ею как новые, так и уже существующие услуги.

10.4.2. Определение

Определение области (диапазона)¹ и глубины требований заказчика рассматривается как процесс дизайна (разработки) в рамках Процесса Управления Уровнем Сервисов. Согласно модели обеспечения качества стандарта ISO 9001 общий процесс дизайна состоит из следующих этапов: собственно дизайн, разработка, инсталляция и сопровождение. Для того чтобы результаты выполнения процесса дизайна отвечали требованиям заказчика, им необходимо управлять. На протяжении всего процесса дизайна термин «внешний» используется в отношении взаимоотношений с заказчиком, а «внутренний» — с технической поддержкой внутри ИТ-организации. Процесс дизайна включает в себя шаги, начиная с детализации требований заказчика и определения их в качестве стандартов и заканчивая разработкой технических условий для предоставления услуг.

Определение внешних стандартов

Первым этапом в составлении количественного описания² новых или существующих ИТ-услуг является определение или «переопределение» ожиданий заказчика в отношении услуг в целом. Ожидания заказчика формализуются в Требованиях к Уровню Услуг (SLR), в разработке которых участвует вся организация заказчика. Обычно этот этап считается самой трудной частью Процесса Управления Уровнем Сервисов. Перед началом данного этапа Руководитель Процесса должен подготовиться к встрече с представителями заказчика. Первым вопросом, который следует задать, является: «Какой ИТ-сервис требуется и из каких элементов он должен состоять?» Предоставление сервиса может повлечь за собой использование определенной части инфраструктуры, например, такой как глобальная сеть (Wide Area Network — WAN). Этот сервис может быть частью составной/сложной услуги³, такой как доступ ко всей информационной системе, включая всю инфраструктуру (WAN, LAN, рабочие станции, приложения и т. д.).

Участвующие в этих встречах пользователи должны быть поделены на группы. Руководитель Процесса Управления Уровнем Сервиса составляет список групп пользователей, их требований и полномочий. Следующая информация необходима для определения Требований к Уровню Услуг:

- описание функций, которые должен предоставить запрашиваемый сервис, с точки зрения заказчика;
- время и дни, в которые сервис должен быть доступен;
- требования к непрерывности сервиса;
- ИТ-функции, необходимые для предоставления сервиса;
- ссылки на текущие операционные методы и стандарты качества, которые должны учитываться при определении сервиса;
- ссылки на Соглашение об Уровне Сервиса, которое должно быть модифицировано или заменено там, где это необходимо.

Результатом этапа дизайна является документ, содержащий Требования к Уровню Услуг (Service Level Requirements — SLR) и подписанный Руководителем Процесса и заказчиком. Эти требования еще можно менять, пока соответствующее подразделение работает над разработкой услуги, внедрением и ведет соответствующие закупки. Изменения могут касаться, например,

¹ Scope.

² Quantifying.

³ Composite service.

целесообразности предполагаемых функций и ожидаемых затрат. Каждое такое изменение должно утверждаться обеими сторонами.

Преобразование во внутренние стандарты

На этапе составления спецификаций Требования к Уровню Услуг конкретизируются. Результатом работы на этом этапе будет получение следующей информации:

- однозначное и подробное описание ИТ-услуг и необходимых компонентов;
- спецификация метода внедрения и предоставления сервисов;
- спецификация процедуры контроля требуемого Уровня Качества.

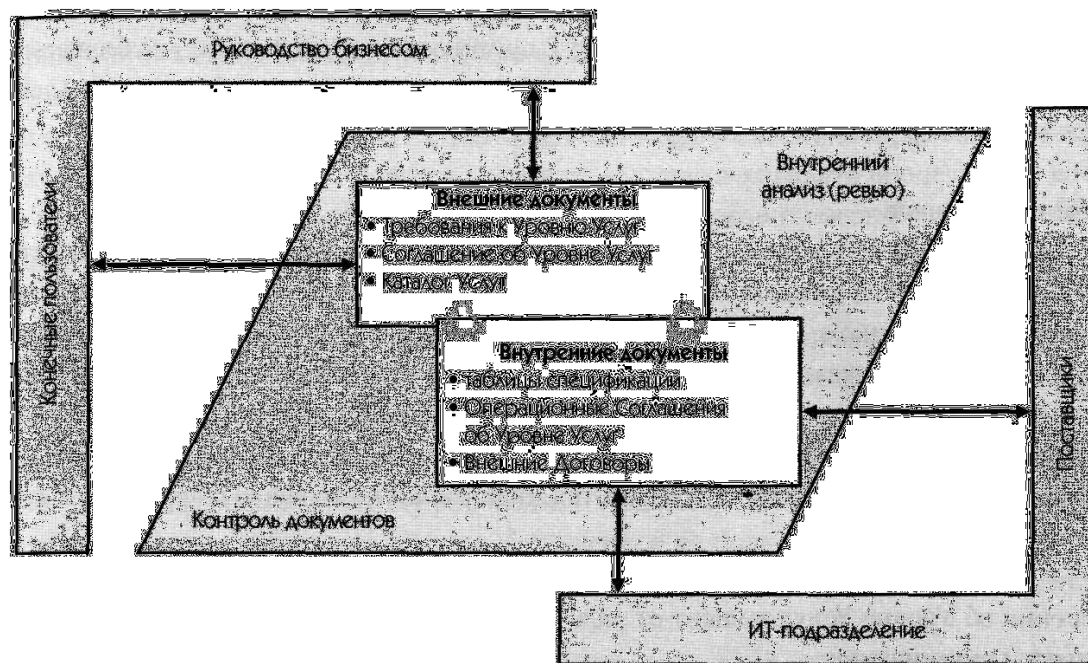


Рис. 10.2. Этап составления спецификаций (источник: OGC)

На этапе составления спецификации рекомендуется разграничивать внешние и внутренние документы (рис. 10.2). Спецификации для внешнего использования уточняют согласованные с заказчиком цели, и контроль процесса дизайна осуществляется с учетом этих целей. Такие спецификации составляются совместно с организацией заказчика, и они служат входной информацией для внутренних спецификаций.

Внутренние спецификации согласуются с внутренними целями ИТ-организации, достижение которых означает удовлетворение потребностей заказчика. Разграничение между внутренними и внешними спецификациями может оказаться особенно полезным уже после того, как Процесс Управления Уровнем Сервиса запущен в работу. При таком подходе ИТ-организация не будет беспокоить заказчика различными техническими вопросами. Начиная с этого момента, Управление Уровнем Сервиса означает стремление поддерживать соответствие внутренних спецификаций внешним. Этому содействуют выполнение таких действий, как Контроль документов и Внутренний анализ (ревью), в ходе которых ведется регистрация относящихся к данному вопросу документов, управление версиями и организуются регулярные аудиторские проверки.

Таблицы спецификаций¹ дают подробное описание того, что хочет заказчик (внешний элемент), и того, как пожелания заказчика отразятся на работе ИТ-организации (внутренний элемент). Таблицы не обязательно должны подписываться двумя сторонами, но все равно они попадают в сферу деятельности по Контролю документов. Каталог услуг может составляться на основе спецификаций сервисов, поэтому любые изменения в Уровнях Услуг должны быть немедленно отражены в Таблице спецификаций и в Каталоге услуг. Вслед за этим пересматривается Соглашение об Уровне Сервиса в соответствии с измененными спецификациями.

¹ Service Specifications (Spec sheets).

План обеспечения качества услуг (Service Quality Plan — SQP)

Рекомендуется включать всю управленческую информацию (Ключевые показатели эффективности) и внутренние и внешние спецификации в единый документ для получения полной информации о вкладе каждого процесса Сервис-менеджмента в ИТ-услуги.

10.4.3 Договор

После завершения этапа составления спецификаций, ИТ-организация трансформирует бизнес-потребности в ИТ-ресурсы и Конфигурационные Элементы. Далее эта информация будет использована для составления или модификации следующих документов.

Соглашение об Уровне Сервиса

При разработке структуры данного документа вначале рекомендуется определить общие аспекты, такие как сетевые услуги для всей компании, и разработать общую сервисную модель соглашений до начала переговоров с заказчиком. Соглашение может иметь иерархическую структуру, аналогичную структуре организации заказчика, и может быть представлено в виде рамочного соглашения с определенным количеством иерархических уровней. У каждого Уровня может быть своя степень детализации. Верхние Уровни отражают договоренности по общим услугам, предоставляемым всей организации. На Нижних Уровнях содержится информация, имеющая отношение к конкретным заказчикам.

Структура Соглашения об Уровне Услуг зависит от ряда переменных, таких как:

- **Физические аспекты организации:**

- размер организации;
- сложность;
- географическое распределение.

- **Аспекты культуры:**

- язык, на котором составляются документы (для международных организаций);
- взаимоотношения между ИТ-организацией и заказчиком;
- политика выставления счетов¹;
- однородность бизнес-деятельности;
- тип организации: коммерческая или некоммерческая.

- **Характер бизнес-деятельности:**

- общие положения и условия;
- часы работы — 5x8 часов или 7x24 часа.

Внешние Договоры и Операционные Соглашения об Уровне Услуг

Все имеющиеся Внешние Договоры (UC) и Операционные Соглашения об Уровне Услуг (OLA) должны быть пересмотрены на этапе дизайна. Участвующие в этой работе должны иметь информацию обо всех соглашениях OLA и договорах UC, которые относятся к предоставлению конкретной услуги. Ссылки в результате деятельности по Контролю документов могут помочь в уточнении связей с таблицами спецификаций.

Каталог услуг

При составлении Каталога услуг могут быть полезны следующие рекомендации:

- используйте язык заказчика. Избегайте технического жаргона и используйте терминологию из соответствующей области бизнеса;
- постарайтесь взглянуть на проблему с точки зрения заказчика и придерживайтесь такого подхода при сборе нужной информации;

¹ Charging

- создайте привлекательный макет каталога, так как ИТ-организация использует этот документ для своей презентации заказчикам;
- постарайтесь сделать этот документ доступным для наибольшего количества потенциальных заинтересованных лиц, например, путем опубликования его на сайте сети Интранет или на CD-ROM.

10.4.4. Мониторинг

Мониторинг Процесса Управления Уровнем Сервиса можно проводить, только если Уровни Услуг заранее четко определены и соответствуют внешним целям. Также должна существовать возможность измерения Уровня Услуг с точки зрения заказчика. Мониторинг не должен ограничиваться техническими аспектами процесса, он также должен затрагивать процедурные вопросы. Например, до тех пор, пока пользователь не будет проинформирован о восстановлении сервиса, он будет считать его недоступным.

Процессы Управления доступностью и мощностями обычно предоставляют информацию о достижении технических целей, связанных с Уровнями Услуг. В некоторых случаях информация также поступает из Процессов Поддержки услуг, особенно от Процесса Управления Инцидентами. Однако недостаточно замерять только внутренние параметры, так как это не даст представления о восприятии услуг заказчиком. Поэтому необходимо замерять/оценивать и такие параметры, как время реагирования, время эскалации и время, затраченное на поддержку. Полное представление о процессе можно получить только путем объединения информации, получаемой как от систем, так и от Сервис-менеджмента.

10.4.5. Создание отчетов

Отчеты заказчику (отчеты о сервисах) должны предоставляться в сроки, оговоренные в Соглашении SLA. В этих отчетах сравниваются фактически предоставляемые Уровни Сервисов с согласованными Уровнями. Примерами отчетов могут быть:

- доступность сервисов и время простоя в указанные периоды;
- среднее время реагирования в пиковые периоды;
- скорость транзакций в пиковые периоды;
- количество функциональных ошибок в ИТ-сервисе;
- частота и длительность периода деградации сервисов (Услуги не достигают согласованного Уровня);
- среднее количество пользователей в пиковые периоды;
- количество успешных и безуспешных попыток нарушить систему безопасности;
- количественное соотношение использованных мощностей¹ сервисов;
- количество завершенных и незавершенных (открытых) изменений;
- стоимость предоставленных услуг.

10.4.6. Анализ (ревью)

Уровень Сервисов нужно регулярно анализировать, уделяя при этом внимание следующим аспектам:

- Соглашению об Уровне Услуг с момента последнего анализа;
- проблемам, возникшим с услугами;
- выявлению тенденций работы услуг;
- изменению услуг в пределах Согласованных Уровней Сервиса;
- изменению процедур и расчетов стоимости дополнительных ресурсов;
- последствию сбоев при предоставлении Согласованных Уровней Услуг.

¹ Capacity.

Если не удалось организовать предоставление ИТ-услуг на Согласованном Уровне, следует согласовать действия по исправлению ситуации, например:

- разработать Программу улучшения услуг (Service Improvement Program — SIP);
- выделить дополнительный персонал и ресурсы;
- изменить Уровни Сервисов, определенные в Соглашении SLA;
- модифицировать процедуры;
- модифицировать Соглашения OLA и Внешние Договоры UC.

Во многих организациях, в которых вводится Процесс Управления Уровнем Сервисов, ведутся обсуждения, требуется ли определение санкций в связи с несоблюдением договоренностей. Это трудный вопрос, поскольку Процесс Управления Уровнем Сервиса базируется на взаимодействии ИТ-подразделения с пользователями ИТ-услуг, часто в рамках одной организации. В такой ситуации, когда и ИТ-подразделение, и пользователи работают над достижением одних и тех же корпоративных целей, маловероятно, чтобы применение санкций и тем более денежных штрафов отвечало бы корпоративным интересам. Было бы намного разумнее, исходя из общих интересов, договориться о совместных мерах по предотвращению сбоев в предоставлении Согласованных Уровней Услуг. Тем не менее возможно применение санкций в отношении внешнего поставщика. В этом случае, скорее всего, нужно заключать юридически обязывающий договор (Внешний Договор), а не Соглашение об Уровне Сервиса.

10.5. Контроль процесса

Для оптимизации процесса и его контроля следует определить ряд критических факторов успеха, а также показателей качества для оценки и улучшения процесса.

10.5.1. Критические факторы успеха и ключевые показатели эффективности

Успех Процесса Управления Уровнем Сервиса зависит от следующих факторов:

- наличия Руководителя Процесса, обладающего знаниями как в области информационных технологий, так и в области бизнеса;
- четкости в формулировании целей процесса и роли процесса;
- проведения оповещения, в ходе которого люди получают информацию о процессе, будет достигнуто его понимание и поддержка с их стороны;
- четкости поставленных задач, полномочий и ответственностей в рамках процесса, разграничения контроля процесса и операционных задач (контактов с заказчиками).
- Приведенные ниже показатели качества можно использовать для определения эффективности и результативности¹ Процесса Управления Уровнем Сервисов:
 - параметры сервисов, включенные в Соглашения SLA;
 - параметры Соглашения SLA, поддерживаемые Операционным Соглашением об Уровне Услуг (OLA) и Внешними Договорами (UC);
 - параметры Соглашений SLA, за которыми ведется мониторинг, и о недостатках которых составляются отчеты;
 - параметры Соглашений об Уровне Сервиса, которые регулярно анализируются;
 - параметры Соглашений об Уровне Сервиса, для которых удалось достичь согласованных уровней сервиса;
 - выявленные недостатки, включенные в план улучшений;
 - действия, предпринятые по исправлению указанных недостатков;
 - выявленные тенденции с учетом реального Уровня Сервиса.

¹ Effectiveness and efficiency

10.5.2. Отчеты руководству¹

Отчеты руководству в отличие от Отчетов об Уровне Сервисов предназначены не для заказчика, они нужны для целей контроля или Управления Процессом. В них могут входить метрики о реально существующих Уровнях Сервисов и сведения о тенденциях, например:

- количество заключенных Соглашений SLA;
- количество случаев несоблюдения заключенных соглашений SLA;
- стоимость оценки и мониторинга Соглашений SLA;
- степень удовлетворенности заказчиков, определяемая по результатам опросов;
- статистические данные об инцидентах, проблемах и изменениях;
- результаты предпринимаемых действий по улучшению сервисов.

10.5.3. Функции и роли

Роли

Контроль за Процессом Управления Уровнем Сервиса осуществляет Руководитель Процесса. Он должен обеспечить эффективность процесса и достижение заданных результатов. Это не обязательно означает, что роль Руководителя Процесса обязательно исполняет один человек. Во многих организациях есть несколько Руководителей Процесса Управления Уровнем сервисов, каждый из которых отвечает за одну или несколько услуг или групп заказчиков.

Ответственность

Руководитель Процесса Управления Уровнем Сервиса отвечает за:

- создание и обновление Каталога Услуг;
- создание и поддержание эффективного Процесса Управления Уровнем Сервисов, включая:
 - определение структуры Соглашения об Уровне Сервиса;
 - заключение Операционных Соглашений об Уровне Услуг с Внутренними Поставщиками;
 - заключение Внешних Договоров с Поставщиками;
- обновление существующей Программы улучшения услуг;
- ведение переговоров с заказчиками, заключение и поддержка Соглашений об Уровне Сервиса, Операционных Соглашений об Уровне Услуг и Внешних Договоров;
- анализ качества работы ИТ-организации и улучшение качества по мере необходимости.

10.6. Проблемы и затраты

10.6.1. Проблемы

В процессе работы могут возникнуть следующие проблемы:

- В результате внедрения Процесса Управления Уровнем Сервиса установились деловые отношения с заказчиком, что требует привлечения всего ИТ-персонала к работе по заключенным соглашениям. В этой ситуации, возможно, потребуется изменение корпоративной культуры в компании.
- Заказчикам может потребоваться помощь в составлении Требований к Уровню Сервисов.
- Может оказаться очень трудным представить ожидания заказчиков в виде поддающихся оценке стандартов и конкретных цифр расходов.
- Руководитель Процесса должен быть умеренным и реалистичным в своих обещаниях при обсуждении соглашений, пока не будут разработаны инструментарии, процедуры, План обеспечения качества услуг (SQP) и Внешние Договоры. Лучше придерживаться стратегии постепенных улучшений.

¹ Management reports.

- Легко ошибиться в расчетах накладных расходов, связанных с мониторингом и оценкой Уровней Сервисов. В больших организациях может потребоваться отдельный персонал на выполнение этих видов работ.
- На практике многие ИТ-организации приступают к составлению проекта Соглашения об Уровне Сервиса, пропуская этап анализа требований заказчика, этап дизайна и разработки Плана обеспечения качества сервисов (SQP). Это может привести к возникновению процесса, которым трудно управлять и у которого нет четких, поддающихся оценке стандартов.
- Документы, появляющиеся в рамках Процесса Управления Уровнем Сервиса и сам процесс могут стать самоцелью вместо достижения цели процесса — стать средством установления хороших отношений между заказчиком и поставщиком ИТ-сервисов.

10.6.2. Затраты

Расходы, связанные с внедрением Процесса Управления Уровнем Сервисов, можно разделить на следующие категории:

- расходы на персонал (Руководитель Процесса и команда проекта);
- расходы на обучение;
- расходы на документацию;
- расходы на помещение, аппаратное и программное обеспечение;
- расходы на операционные виды деятельности, связанные с обновлением Плана Обеспечения Качества Сервисов (SQP), Соглашений об Уровне Сервиса и Каталога Услуг.

Глава 11

Управление Финансами ИТ

11.1. Введение

Для большинства людей ИТ-услуги являются необходимой поддержкой повседневной деятельности, но мало кто понимает, что эти услуги стоят денег. По мере роста числа пользователей растет и бюджет ИТ. С увеличением бюджета заказчиков все больше начинают беспокоить расходы на ИТ, и становится все труднее без посторонней помощи соотнести эти расходы со своей деятельностью. При оплате счета за ИТ-услуги заказчику бывает трудно самому без посторонней помощи определить, насколько реальные затраты окупаются полученными бизнес-преимуществами.

Библиотека ИТЛ создавалась с целью содействовать структурированию Управления ИТ-инфраструктурой, что способствовало бы эффективному и экономичному использованию ИТ-ресурсов. При этом одной из задач было обеспечить переход от организаций, ориентированных в своей деятельности на фиксированный бюджет, к организациям коммерческого типа, которые имеют четкое представление о всех своих затратах.

Качество и затраты

Предоставление ИТ-услуг пользователям по разумной цене определяется тремя факторами:

- Качество — в плане операционной деятельности¹:
 - мощность (пропускная способность);
 - доступность;
 - производительность;
 - восстановление после чрезвычайных обстоятельств;
 - поддержка.
- Стоимость — в плане:
 - расходов;
 - инвестиций.
- Требования заказчика — стоимость и качество должны соответствовать потребностям бизнес-пользователя.

Первые два фактора часто находятся в противоречии друг с другом, так как повышение качества обычно означает увеличение затрат, а уменьшение затрат означает снижение качества. Однако эти два фактора могут быть сбалансированы за счет четкой ориентации на потребности заказчика. Осведомленность о затратах, связанных с предоставлением ИТ-услуг, и использование реалистичной системы выставления счетов ставит предоставление услуг на прочную основу. Это позволяет заказчикам быть в курсе стоимости ИТ-услуг, они будут знать, что с них запрашивают разумную цену, и, как следствие, они будут разумнее использовать ИТ-ресурсы.

11.1.1. Основные понятия

Составление бюджета

Составление бюджета включает в себя прогнозирование затрат и контроль расходов. Часто этот процесс начинается с планирования потребностей заказчика в услугах и связанных с этим затрат. Прогноз может составляться на основе анализа накопленных статистических данных с возможными поправками на текущие тенденции в бизнесе и с учетом персональных знаний специалиста, составляющего бюджет. Если статистические данные по конкретной услуге отсутствуют, то в качестве модели можно использовать аналогичные сервисы.

¹ Operations.

Бухгалтерский учет

Бухгалтерский учет – это мониторинг расходования финансовых средств ИТ – организацией. Здесь особенно важным является определением затрат по каждому заказчику, по каждому виду услуг, деятельности и т.д. В данном случае понимание вопроса в целом более важно, чем возможность рассчитать стоимость до копейки.

Выставление счетов

К выставлению счетов относятся все виды деятельности, связанные с подготовкой счетов заказчикам за предоставленные услуги. Данный процесс предполагает определение цели (целей) выставления счетов, а также алгоритма (алгоритмов) расчета стоимости¹. Для этого необходима эффективная система бухгалтерского учета, удовлетворяющая потребностям в детальной информации на различных уровнях: анализа, расчета и отчетности.

Категории затрат

Эффективный контроль уровня затрат требует понимания их природы. Существует несколько способов классификации затрат.

Для каждого продукта или сервиса можно определить затраты, прямо или косвенно связанные с ним:

- **Прямые затраты**²: затраты, связанные конкретно и исключительно с какой – либо ИТ – услугой. Например, виды деятельности и материалы, прямо и однозначно связанные с определенным сервисом (аренда телефонной линии для доступа к сети Интернет).

- **Косвенные затраты**³: затраты, не связанные прямо и однозначно с какой – либо ИТ – услугой. Примерами могут быть затраты на помещения, услуги по поддержке (например, Управление Сетью) и административные расходы (включая затраченное время).

Одним из способов включая косвенных затрат в счет является их пропорциональное распределение между услугами или заказчиками.

Другим способом является расчет затрат на основе деятельности (Activity Based Costing – ABC). Этот метод заключается в учете всех накладных расходов организации с последующим распределением затрат на выполнение работ по продуктам и услуг, с которыми эти затраты связаны.

В сущности, затраты распределяются по более сложному критерию, чем простое распределение прямых затрат. Метод ABC может быть полезен в тех случаях, когда большинство затрат не зависит напрямую от объема услуг. Вместо усредненного распределения косвенных затрат метод ABC предлагает распределять их на основе выполненной деятельности, связанной с конкретным продуктом и услугой.

Еще одним способом учета затрат является их разделение на постоянные и переменные.

- **Постоянные затраты**⁴ не зависят от объема предоставляемых услуг, к ним относятся инвестиции в аппаратное обеспечение, программное обеспечение и строительство. В большинстве случаев учитывается не закупочная цена, а ежемесячная или ежегодная сумма амортизационных отчислений и начисляемые проценты. Постоянные затраты присутствуют даже при снижении объема производства (предоставления услуг) или их прерывания.

- **Переменные затраты**⁵ – это затраты, уровень которых меняется с изменением объема производства. Примерами могут быть затраты на привлекаемый со стороны персонал, картриджи для принтеров, бумагу, отопление и электричество. Эти затраты связаны с предоставляемыми услугами; с увеличением объема производства возрастают также и затраты.

Существует определенное различие между капитальными и операционными затратами.

¹ Charges.

² Direct costs.

³ Indirect costs.

⁴ Fixed costs.

⁵ Variable costs.

• **Капитальные затраты**¹ связаны с закупкой активов, предназначенных для долгосрочного использования внутри организации. Амортизация этих затрат производится в течение нескольких лет. Поэтому в затраты обычно включаются амортизационные отчисления, а не закупочная стоимость.

• **Операционные затраты**² представляют собой ежедневные затраты, не связанные с материальными производственными ресурсами. Примерами являются договоры на обслуживание аппаратного и программного обеспечения, стоимость лицензий, страсовые взносы и т.д.

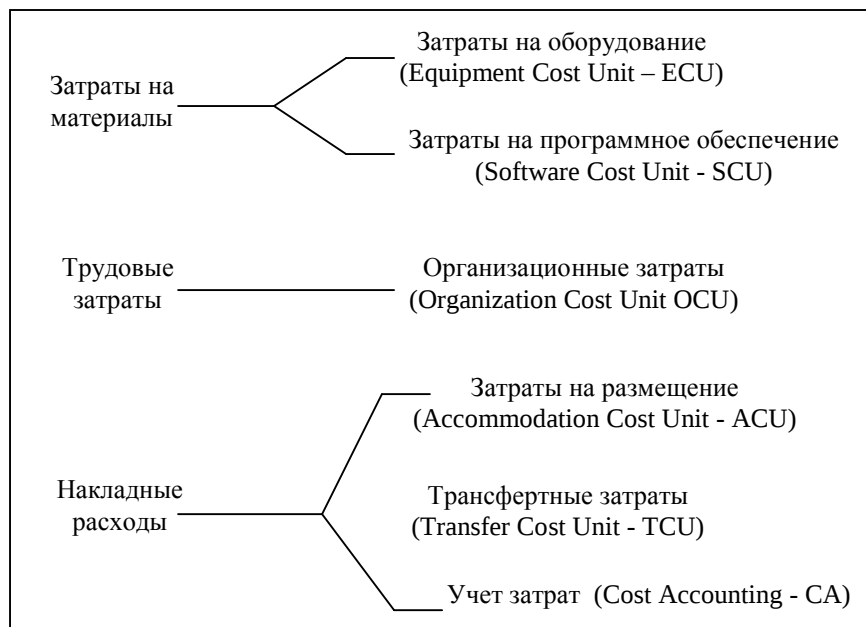


Рис. 11.1. Типы затрат и их составляющие (источник: OGC)

Типы затрат (виды затрат)

После определения структуры калькуляции затрат (например, по подразделениям, услугам или заказчикам), может быть определена система типов затрат для разнесения затрат по счетам. Число типов будет зависеть от размера организации. Типы затрат должны иметь четкое и понятное описание и структуру, чтобы не возникло трудностей при их распределении.

Типы затрат могут быть также подразделяться на элементы затрат. Методы распределения затрат по ним могут быть определены на более позднем этапе. Существует шесть основных видов затрат, относящихся или к прямым, или к косвенным затратам.

Примерами этих видов затрат могут быть:

• **Затраты на оборудование (Equipment Cost Unit – ECU)** – все затраты на аппаратное обеспечение, например:

- серверы;
- устройства хранения информации;
- связь и сети;
- принтеры.

• **Затраты на программное обеспечение (Software Cost Unit – SCU)** – прямые и косвенные затраты на поддержание функционирования системы, включая:

- системное программное обеспечение;
- транзакционную систему;
- систему Управления Базами Данных;
- систему разработки приложений;
- программные приложения.

• **Организационные затраты (Organization Cost Unit — OCU)** — прямые и косвенные затраты на персонал, которые могут быть постоянными или переменными, например:

- заработная плата;

¹ Capital costs.

² Operational costs.

- расходы на обучение;
- командировочные расходы.
- **Затраты на размещение (Accommodation Cost Unit — ACU)** — все прямые и косвенные затраты, связанные с размещением, например:
 - серверные комнаты;
 - офисы;
 - другие помещения и оборудование, такие как испытательные лаборатории, учебные помещения, кондиционеры и т. д.
- **Трансферные затраты (Transfer Cost Unit — TCU)** — затраты, связанные с товарами и услугами, предоставляемыми другими подразделениями, т. е. внутренние расчеты между подразделениями организации.
- **Учет затрат (Cost Accounting — CA)** — затраты, связанные с деятельностью самого Процесса Управления Финансами.

11.2. Цели процесса

Целью Процесса Управления Финансами является содействие ИТ-организации в эффективном Управлении ИТ-ресурсами, необходимыми для предоставления услуг. Для этого в рамках процесса выполняется разбиение общих затрат на составляющие части и их распределение по предоставляемым ИТ-услугам. Таким образом процесс обеспечивает поддержку принятия решений по вопросам инвестиций и способствует разумному пользованию ИТ-средств с учетом их стоимости.

Для выставления счетов может быть выбран метод, нацеленный на полное возмещение затрат, на возмещение с учетом дополнительного финансирования (предусмотренного в бюджете), или на возмещение с целью получения определенной прибыли.

Преимущества использования процесса

При внедрении ИТ-организацией процесса Управления Финансами она получит возможность:

- определять затраты на ИТ-услуги;
- определять и классифицировать структуру затрат;
- правильно распределять затраты по ИТ-услугам, предоставляемым внутренним и внешним заказчикам;
- использовать различные методы выставления счетов за пользование ИТ-услугами, где это целесообразно;
- управлять ИТ-отделом как бизнес-подразделением, где это требуется;
- возмещать все расходы, включая капитальные затраты (инвестиции, амортизационные отчисления и банковские проценты) за счет заказчика;
- регулярно проверять счета на предмет их реалистичности и приемлемости для заказчика;
- формировать поведение заказчиков и пользователей путем уведомления их о затратах и привязывания затрат непосредственно к услугам.

Так как преимущества различны по своей природе, то делается разграничение между работами по Составлению бюджета¹, Ведению бухгалтерского учета² (который участвует в Расчете затрат³) и Выставлением счетов⁴.

Главное достоинство деятельности по **Составлению бюджета и Ведению бухгалтерского учета** состоит в том, что это дает руководству более полную информацию о затратах на

¹ Budgeting.

² Accounting.

³ Costing.

⁴ Charging.

предоставление ИТ-услуг. Такая информация позволяет сбалансировать затраты и качество и обеспечить заказчикам финансово-обоснованный ИТ-сервис.

Бюджетирование и ведение бухгалтерского учета позволяет руководителю ИТ-сервисов:

- принимать решения по каждой услуге на основе экономической эффективности;
- использовать коммерческий подход к принятию решений по ИТ-услугам и инвестициям в них;
- предоставлять больше информации для обоснования расходов, например, показывая возможные издержки в случае отказа от стратегических затрат;
- составлять бюджеты и планы на основе надежной информации.

Основным достоинством системы **Выставления счетов** является содействие развитию деловых отношений с заказчиком. Оплачивающий услуги заказчик имеет соответствующие права и может выдвигать требования, но он будет использовать ресурсы более экономно, если будет понимать связь между выдвигаемыми им требованиями и получаемым счетом за услуги.

Выставление счетов позволяет ИТ-руководству:

- анализировать ИТ-услуги с коммерческой точки зрения и планировать инвестиции на основе принципа возмещения затрат;
- возмещать затраты на ИТ, увязывая их с получаемой от услуг пользой;
- влиять на поведение заказчика, например, назначая более высокие тарифы в периоды максимальной загрузки или просто предоставляя руководству информацию о стоимости и использовании услуг для принятия мер.

Использование системы Выставления счетов должно способствовать формированию поведения заказчика, а не создавать ситуацию, при которой заказчик за плату получает все, что хочет. Вряд ли возможно удовлетворить индивидуальные требования всех пользователей по индивидуальным расценкам, даже если они готовы платить. Система выставления счетов создает коммерческую среду для переговоров. В этом случае заказчики будут лучше осведомлены о затратах, связанных с использованием ИТ-средств.

11.3. Процесс

В последние годы роль информационных технологий значительно возросла. Поэтому ИТ-организации столкнулись с возросшими требованиями к качеству и экономической эффективности ИТ-услуг. Развитие Интернета привело к тому, что ИТ-организации все чаще приходится иметь дело с внешними, по отношению к компании заказчиками и пользователями. Например, книжные магазины размещают свои каталоги в Интернете и обслуживают заказчиков по всему миру. Это приводит к расширению масштаба организации и необходимости получать более точную информацию о затратах. Для обеспечения рентабельности ИТ-сервиса необходимо также наличие соглашения о предоставлении услуг и определение разумных цен. ИТ-организации в своей деятельности должны применять бизнес-ориентированный стиль работы, и внедрение эффективной системы контроля затрат является частью такого подхода. Эффективная система контроля затрат должна отвечать следующим требованиям:

- поддерживать разработку инвестиционной стратегии, способствующей гибкости предприятия за счет использования современных технологических средств;
- помогать в определении приоритетов в использовании ресурсов;
- обеспечивать покрытие затрат на все используемые организацией ИТ-ресурсы, включая обновление информации;
- помогать руководству в принятии ежедневных оперативных решений, что позволит уменьшить финансовый риск при принятии долгосрочных решений;

- быть гибкой и способной быстро реагировать на изменения в бизнесе.

Процесс Управления Финансами оказывает поддержку бизнесу в планировании и достижении поставленных целей. Для получения наиболее оптимального результата от использования данного процесса он должен применяться постоянно в масштабе всей компании, с минимумом конфликтных ситуаций. В ИТ-организации процесс Управления Финансами реализуется через три основных процесса: Составление бюджета (Budgeting), Бухгалтерский учет (Accounting) и Выставление счетов (Charging). Этот цикл показан на рис. 11.2.

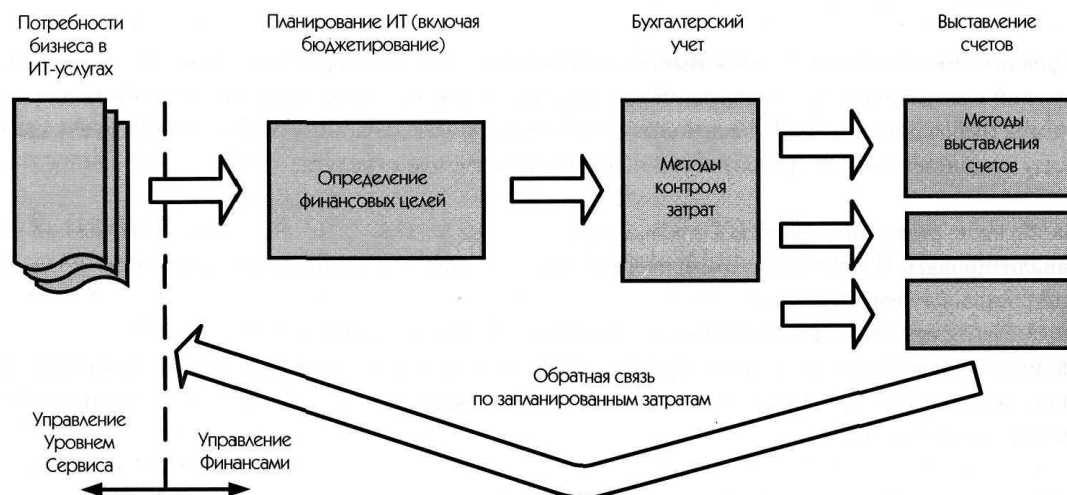


Рис. 11.2. финансовый цикл (источник: OGC)

Процесс Управления Финансами ИТ-услуг взаимодействует почти со всеми другими процессами ИТ Сервис-менеджмента, но в особенности с приведенными ниже.

Взаимоотношения с бизнес-процессами

Управления Уровнем Сервиса имеет большое значение для определения концепции, стратегии и планирования в соответствии с бизнес-процессами (рис. 11.3).

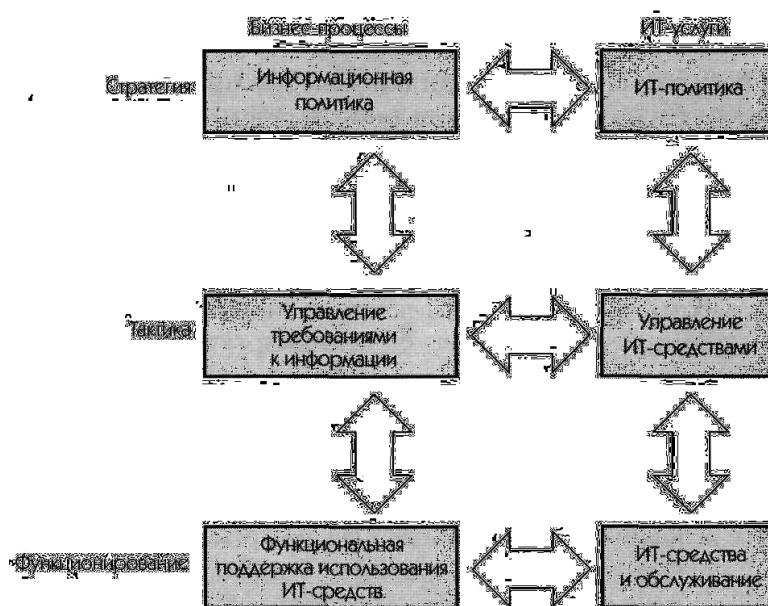


Рис. 11.3. Взаимоотношения с бизнес-процессами

Хотя эти виды деятельности находятся вне сферы действия Процесса Управления Финансами, они важны для него. Это объясняется тем, что бизнес имеет концепцию действий на будущее, которая учитывается при определении реальных задач как для всех бизнес-подразделений, так и для самой ИТ-организации.

Следовательно, стратегия ИТ должна основываться на задачах бизнеса. По мере того, как ИТ-организация будет все больше узнавать о целях и задачах бизнеса, будет появляться больше возможностей для эффективного использования новых информационных технологий. Затраты на внедрение и эксплуатацию ИТ-решений должны оцениваться по тому, насколько ИТ-технологии способствуют достижению бизнес-преимуществ в терминах снижения операционных затрат и увеличения оборота.

Взаимоотношение с Процессом Управления Уровнем Сервиса

Соглашение об Уровне Сервиса (SLA) определяет ожидания заказчика и соответствующие обязательства ИТ-организации. Вид и объем услуг во многом определяются финансовыми ресурсами, выделяемыми для предоставления этих услуг. Руководитель Процесса Управления Финансами ИТ-организации участвует в обсуждении с руководителем Процесса Управления Уровнем Сервиса таких вопросов, как затраты на удовлетворение текущих и будущих требований бизнеса, политика компании в области выставления счетов и ее влияние на заказчика и его поведение.

Чем больше различных уровней услуг для различных заказчиков предусматривается в Соглашении SLA, тем большее значение для ИТ-сервиса приобретает процесс выставления счетов и тем весомее будут получаемые преимущества. Но это также ведет к увеличению накладных расходов, связанных с составлением бюджета, ведением бухгалтерского учета и процедурой выставления счетов.

Взаимоотношения с Процессом Управления Мощностями

Мощности ИТ сервисов и уровень их доступности зависят от выделяемых финансовых ресурсов. Может возникнуть необходимость обсудить дополнительные затраты на предоставление улучшенных мощностей и повышенной доступности с заказчиком ИТ-услуг или со всей компанией в целом. Информация о соотношении между стоимостью услуг и бизнес-отдачей может повлиять на принятие решения о целесообразности приобретения дополнительных мощностей или увеличение уровня доступности.

Взаимоотношения с Процессом Управления Конфигурациями

Процесс Управления Конфигурациями определяет, идентифицирует и регистрирует все изменения во всех компонентах инфраструктуры. Использование информации, включая данные о затратах из конфигурационной базы данных CMDB, облегчает сбор статистической информации о стоимости услуг. Процесс Управления Конфигурациями может также участвовать в сверке данных об активах с информацией из финансовых систем.

11.4. Виды деятельности

11.4.1. Составление бюджета

Задачей подпроцесса Составления бюджета является планирование деятельности организации и ее контроль. В то время как корпоративное и стратегическое планирование учитывает долгосрочные бизнес-задачи, бюджетирование определяет финансовые планы для поставленных задач на заданный бюджетный срок. Обычно такой период составляет от одного года до пяти лет¹.

Методы составления бюджета

В зависимости от финансовой политики бизнеса выбирается один из следующих методов:

¹ По мнению редакторов, в настоящее время для ИТ этот период составляет 6-12 месяцев, при периоде долгосрочного планирования около 3-х лет.

- **Инкрементное (приростное) составление бюджета** — в качестве основы для нового бюджета используются цифры за прошлый год. Они корректируются в соответствии с ожидаемыми изменениями в деятельности организации, затратах и ценах.

- **Составление бюджета «с нуля»** — работа над бюджетом начинается с чистого листа бумаги «с нуля». Опыт прошлых лет не принимается в расчет. Это заставляет руководителей определять все потребности в ресурсах с учетом затрат, заложенных в их бюджеты. Это означает, что каждая статья расходов должна быть проанализирована и принято решение об их целесообразности и величине. Очевидно, что этот метод более трудоемкий, поэтому обычно он используется раз в несколько лет. В промежутках используется метод инкрементного составления бюджета.

Составление бюджета

Составление бюджета начинается с определения ключевых факторов, сдерживающих рост компании. Во многих случаях это объем продаж; однако, этими факторами могут также быть недостаток складского пространства, материалов и т. д. Часто бюджет определяют финансовые ограничения. Процесс составления включает в себя определение следующих вторичных бюджетов (мы опускаем процедуры согласования и утверждения, существующие в каждой компании):

- **Бюджет отдела продаж и маркетинга** — если бюджет определяется объемом продаж, то большая часть работы ложится на отдел маркетинга. Для составления хорошего бюджета крайне необходимы точная оценка и анализ заказчиков, рынков, регионов сбыта, продуктов и т. д.

- **Производственный бюджет** — включает подробную информацию о предоставляемых услугах: количество, время поставки, необходимые затраты рабочей силы и материалов и т. д.

- **Административные бюджеты** — исходя из планируемых услуг необходимо определить бюджет на накладные расходы для соответствующих отделов, например, производственного отдела, отделов продаж и распространения, исследований и разработок и т. д.

- **Бюджет на затраты и инвестиции** — этот бюджет складывается из затрат, заложенных в вышеуказанные бюджеты. Бюджет инвестиций определяет расходы, связанные с заменой и приобретением средств производства. В нем могут также учитываться инвестиционные проекты, начатые в прошлом году.

Бюджетный период

Лучшим выбором для бюджетного периода является финансовый год. Для проведения регулярного сопоставления фактических и запланированных в бюджете цифр бюджетный период делится на месяцы или другие равные промежутки времени, например, четырехнедельные периоды.

В некоторых видах бизнеса составляется не только подробный годовой бюджет, но и делается общий прогноз на три года или пять лет. Такой прогноз дает высшему руководству информацию о перспективах на более длительный период.

11.4.2. Бухгалтерский учет

Для того чтобы иметь возможность руководить ИТ-организацией как бизнес структурой, необходимо определять и понимать все затраты, связанные с использованием ИТ. Затраты должны быть определены, даже если соответствующий счет не выставляется заказчику. Контроль затрат возможен только при их четком понимании. Здесь не столько важно определить второстепенные затраты, сколько определить способы структурирования затрат. Это дает лучшее понимание путей расходования денег.

Одной из главных операций бухгалтерского учета является определение элементов затрат. Такая структура затрат определяется на один год, после чего она может быть пересмотрена. В большинстве случаев метод учета затрат выбирается в момент согласования структуры

элементов затрат с бизнес-руководством. Поэтому она должна быть совместима с методами, используемыми в компании. Во многих случаях затраты учитываются по каждому подразделению, заказчику или продукту. Однако в идеале структура должна отражать предоставляемые услуги. Даже если этот процесс не используется при выставлении счетов, ИТ-организация может посчитать полезным создать структуру затрат на основе структуры сервисов, определенных в Каталоге Услуг.

На рис. 11.4 показан пример иерархической структуры сервисных элементов, определенных ИТ-организацией для предоставления услуг. В этой структуре сервисные элементы нижнего уровня поддерживают элементы более высокого уровня. Чем выше положение элемента в структуре, тем выше его значимость для бизнеса.

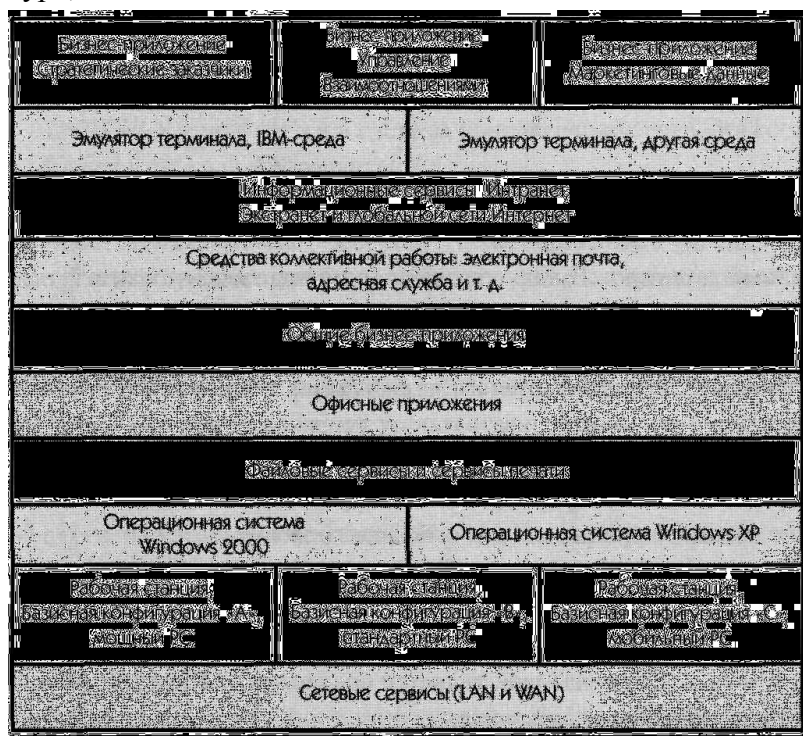


Рис. 11.4. Пример структуры сервиса

После определения сервисных элементов необходимо определить элементы затрат, которые затем подразделяются на единицы затрат, такие как персонал, аппаратное, программное обеспечение, накладные расходы и т. д.

Преимущество структурирования элементов затрат в соответствии с элементами сервиса заключается в том, что становятся отчетливо видны расходы на аппаратное, программное обеспечение и поддержку услуг. В дополнение к структуре прямых затрат, показанной на рис. 11.4, возможно, компания примет также решение о распределении косвенных затрат по услугам. Чем более детализированной будет структура сервиса, тем легче будет понять распределение затрат. В качестве альтернативы в каталоге могут быть указаны только три стандартных рабочих станции, которые включают в себя все. В этом случае в схеме будет только три столбца и гораздо меньше элементов затрат. Такая структура может быть проще для понимания, но при этом уменьшится уровень детализации информации. Например, может быть непонятно, на какой элемент должны быть распределены затраты на поддержку сети, из-за чего будет невозможно определить необходимый для нее уровень поддержки.

Далее составляются бюджеты на следующий год по каждому элементу сервиса и затрат на основе прошлого опыта и с учетом предварительной оценки роста в следующем году. Производится ежемесячный мониторинг бюджетов с целью выявления изменений, таких как непредвиденный рост, и, в случае необходимости, для приведения бюджетов в соответствие с развитием бизнес-ситуации.

11.4.3. Выставление счетов

Ведение учета затрат, безусловно, не является новшеством, но оно приобретает все большее значение. При этом выставление счетов за внутренние затраты — это относительно новое явление, которое является эффективным средством поощрения пользователей к экономному использованию ИТ-ресурсов. Однако взимание платы за ИТ-услуги не принесет много пользы, если держатели бюджета в компании не будут оплачивать другие услуги, такие как телефон, помещение, почтовые услуги, питание, управление кадрами и т. д. Другими словами, практика выставления счетов должна соответствовать финансовой политике организации. Если такая практика существует, то держатели бюджета могут осуществлять управление текущими затратами, которые возможно включать в цену их продуктов и услуг.

Обычно практику выставления счетов вводят для возмещения всех возникающих затрат. В этом случае ИТ-организация работает как бизнес-подразделение компании. Но это осуществимо только в том случае, если известны реальные текущие затраты на ИТ-услуги.

Политика выставления счетов

Прежде чем определить тариф на услуги, рекомендуется проанализировать возможные варианты выставления счетов и определить политику в этой области.

Существуют несколько вариантов такой политики. Выбор подходящего метода зависит от целей, стоящих перед Процессом Управления Финансами. В то же время, если выставление счетов вводится поэтапно, то на каждом этапе могут использоваться различные правила. Политика выставления счетов это:

- **Обмен информацией (Коммуникации)** — руководителям, являющимся заказчиками ИТ-услуг, сообщают о тарифах, чтобы они были осведомлены о затратах их подразделений на ИТ-сервисы. Это может быть сделано двумя способами:

- расчет затрат по каждому подразделению¹ и информирование их руководителей;
- то же, но включая выставление счетов с использованием выбранного метода.

- **Гибкость ценообразования** — чаще всего тарифы определяются и затем используются на ежегодной основе. Если поставщик услуг проявляет инициативу по инвестициям в конкретную услугу в связи с ее частым использованием, то в контракт может быть включена статья о выставлении счетов на покрытие дополнительных затрат. Альтернативой является предложение образующейся дополнительной мощности другим потенциальным заказчиком.

- **Условное выставление счетов** — затраты включаются в направляемые заказчику счета, но без требования оплаты. Этот метод позволяет ИТ-организации накопить опыт по использованию процесса и затем исправить ошибки в системе выставления счетов. Это также дает заказчику возможность привыкнуть к практике выставления счетов. Однако такой метод применим только в том случае, если в конце концов затраты действительно будут возмещены, в противном случае информирование о затратах будет бесполезным.

Тарифы²

Часто бывает трудно установить тариф на услугу. Установление тарифов включает следующие действия:

- определение цели выставления счетов;
- определение прямых и косвенных затрат;
- определение тарифов, существующих на рынке;
- анализ спроса на услуги;
- анализ количества заказчиков и конкуренции.

При определении тарифа за услуги организация должна сначала определить цель и ожидаемую выгоду для заказчика и ИТ-персонала.

¹ Business unit.

² Rates.

Цена является одной из четырех составляющих маркетинга, куда входят: продукт, цена, продвижение и место (четыре P: Product, Price, Promotion, Place). Цена имеет значение не только при возмещении затрат, но и при формировании спроса на продукцию. Гибкая стратегия ценообразования может использоваться для продвижения продуктов на рынок или для их снятия. Новая услуга, у которой еще мало заказчиков, может субсидироваться за счет прибыли от продажи других услуг. Перед выбором стратегии ценообразования следует четко определить затраты на услугу.

Существуют разные типы политики ценообразования, например:

- **Издержки плюс фиксированная прибыль** — известно несколько вариантов, общей основой которых является включение в цену затрат плюс чистая прибыль (стоимость + % наценки). Затраты и чистая прибыль могут определяться несколькими способами, такими как:

- все затраты плюс чистая прибыль;

- маргинальные затраты плюс маржа (наценка, достаточная для покрытия средних постоянных затрат, затрат на единицу продукции и стоимости капитала). Например, если доступ к LAN/WAN учитывается в счете за подключение к сети, эта составляющая уже не должна включаться в другие LAN-сервисы;

- один из вышеуказанных способов с маржой в 0%.

- **Существующая ставка** — для услуг, по которым уже существуют ценовые соглашения.

- **Получение целевого дохода** — для услуг, цена которых была определена заранее.

- **Рыночная ставка (допустимая на рынке)** — цены, которые сопоставимы с ценами внешних поставщиков.

- **Согласованная договорная цена** — эти цены согласуются с заказчиком. Если заказчику необходима новая услуга, обсуждается вопрос о том, должна ли цена включать все затраты на инвестиции, или только их часть.

За услуги, на которые может быть снижена цена при увеличении объема, может предоставляться оптовая скидка. С целью Управления Спросом (распределения спроса во времени) могут использоваться специальные тарифы в моменты пиковой загрузки и в периоды низкого спроса.

11.4.4. Отчетность

В зависимости от выбранной политики выставления счетов заказчик может получать либо счет за фактическое использование ИТ-услуг, либо информацию о реальном объеме использованных ИТ-сервисов. О затратах сообщается на регулярных встречах с заказчиком в рамках процесса Управления Уровнем Сервиса. Поэтому Процессу Управления Уровнем Сервиса передается следующая информация:

- затраты на ИТ-услуги в расчете на одного заказчика;
- разница между фактическими и расчетными затратами;
- используемые методы выставления счетов и методы бухгалтерского учета;
- все ценовые споры, их причины и варианты решения.

11.5. Контроль процесса

Бухгалтерский учет для ИТ является частью общей концепции ИТ Сервис-менеджмента, и им управляет руководитель Процесса Управления Финансами. Руководитель отвечает за внедрение и оперативное управление системой бухгалтерского учета и системой выставления счетов и отчитывается перед руководством ИТ. Руководитель Процесса Управления Финансами не обязательно должен быть сотрудником ИТ-организации. Для оптимизации Процесса Управления Финансами могут использоваться отчеты, критические факторы успеха и ключевые показатели эффективности.

11.5.1. Отчеты для руководства

Предоставляемые руководству ИТ регулярные отчеты о Процессе Управления Финансами должны содержать следующую информацию:

- общие затраты на ИТ-услуги и получаемая бизнес-отдача (доход);
- анализ затрат по каждому ИТ-подразделению, аппаратной платформе или другим значимым разделам;
- затраты, связанные с системой Управления Финансами;
- планирование будущих инвестиций;
- возможности снижения затрат.

11.5.2. Критические факторы успеха и ключевые показатели эффективности¹

Перед внедрением Процесса Управления Финансами следует проинформировать пользователей, персонал и руководство ИТ о цели внедрения процесса, затратах, преимуществах и потенциальных проблемах, связанных с данным процессом.

Эффективное внедрение системы выставления счетов зависит от следующих критических факторов успеха:

- пользователи должны знать, за какие услуги им выставляются счета;
- пользователи должны знать, какие методы выставления счетов используются, чтобы они могли контролировать затраты (например, с помощью соглашений или отчетов, составленных в терминах количественно измеримых показателей производительности);
- система мониторинга затрат должна предоставлять подробную информацию о расходах и их обоснование;
- подход ИТ Сервис-менеджмента должен создать сбалансированную систему эффективных ИТ-сервисов, предоставляемых по разумной цене;
- руководство ИТ должно быть хорошо информировано о преимуществах внедрения Процесса Управления Финансами и связанных с этим затратах, и подтвердить серьезность своих намерений в отношении данного процесса;
- Процесс Управления Конфигурациями должен предоставлять необходимую информацию о структуре услуг для организации соответствующей системы бухгалтерского учета.

Следующие ключевые показатели эффективности работ могут быть полезны для контроля процесса:

- точный стоимостной анализ² по предоставляемым услугам;
- удовлетворенность заказчиков используемыми методами выставления счетов;
- достижение ИТ-организацией ее финансовых целей;
- изменение потребления услуг заказчиками;
- своевременность отчетов для Процесса Управления Уровнем Услуг.

11.5.3. функции и роли

В некоторых ИТ-организациях есть свои финансовые руководители, другие заключают соглашения с финансовым отделом, который тесно сотрудничает с руководством ИТ. Как и любой другой процесс, Управление Финансами должно иметь владельца процесса, отвечающего за развитие и поддержку финансовой системы.

Руководитель Процесса Управления Финансами должен работать на равных началах с руководством других процессов и финансовым отделом для выработки основных направлений развития систем Составления бюджета, Бухгалтерского учета и Выставления счетов.

¹ KPI.

² Cost-benefit analysis (CBA).

11.6. Проблемы и затраты

11.6.1. Проблемы

Потенциальные проблемы могут быть следующими:

- деятельность по регистрации и мониторингу затрат часто является совершенно новой областью для ИТ-персонала, по которой существует не так много литературы;
- для мониторинга, калькуляции затрат и выставления соответствующих счетов часто требуется информация о планировании услуг, не относящихся к ИТ, таких как строительство и т. д., по которым трудно достать подробную информацию;
- трудно найти специалистов, знающих как ИТ, так и бухгалтерский учет;
- отсутствие четко сформулированной и документированной стратегии развития информационных систем, что затрудняет определение необходимых инвестиций;
- недостаточное понимание возможностей, предоставляемых процессом для оптимизации взаимодействия между различными подразделениями;
- недостаточно серьезное отношение к процессу со стороны руководства может означать, что процесс не воспринимается организацией всерьез.

11.6.2. Затраты

Затраты на этот процесс можно разделить на две категории:

- административные и организационные затраты, связанные с планированием, внедрением и выполнением процесса;
- затраты на необходимые инструментальные средства, т. е. аппаратное обеспечение, базы данных и прикладное ПО.

Глава 12

Управление Мощностями

12.1. Введение

Задачей Процесса Управления Мощностями¹ является предоставление в нужное время и в экономически эффективной форме необходимых мощностей для обработки и хранения данных, обеспечивая соответствующий баланс мощностей в ИТ-организации. Хорошее Управление Мощностями исключает панические закупки в последнюю минуту или покупку самой большой системы «на всякий пожарный случай». Подобные ситуации дорого обходятся. Многие центры обработки данных, например, постоянно работают с недогрузкой на 30-40% или больше. Это не так плохо, если у вас небольшое количество серверов. Но если у вас сотни и тысячи серверов, как у многих ИТ-организаций масштаба предприятия, то эти проценты означают потерю огромных финансовых средств.

Управление Мощностями отвечает за решение следующих вопросов:

- Оправдываются ли затраты на приобретение мощностей для обработки данных с точки зрения потребностей бизнеса, и используются ли эти мощности наиболее эффективным образом (соотношение стоимости и мощности)?
- Адекватно ли соответствуют имеющиеся мощности как текущим, так и будущим запросам заказчика (соотношение спроса и предложения)?
- Работают ли имеющиеся мощности с максимальной эффективностью (настройка производительности)? Когда точно необходимо устанавливать дополнительные мощности?

Для выполнения задач Процессу Управления Мощностями необходима тесная связь с бизнес-процессами и ИТ-стратегией. Следовательно, данный процесс является как реактивным (измеряющим и улучшающим), так и проактивным (анализирующим и прогнозирующим).

12.1.1. Основные понятия

К важным понятиям по Управлению Мощностями относятся:

- **Управление Производительностью (Performance Management):** измерение, мониторинг и настройка производительности компонентов ИТ-инфраструктуры.
- **Определение технических средств для приложения (Application sizing):** определение мощности аппаратного обеспечения или пропускной способности сети, необходимых для поддержки новых или модифицированных приложений при ожидаемой рабочей нагрузке.
- **Моделирование (Modeling):** использование аналитических или имитационных моделей для определения требующейся для приложений мощности и выработка наилучшего решения. Моделирование позволяет анализировать различные сценарии и задавать вопросы «что если?».
- **Планирование мощностей (Capacity Planning):** разработка Плана по мощностям, анализ текущей ситуации (предпочтительно с использованием сценариев) и прогнозирование будущего использования ИТ-инфраструктуры и ресурсов, необходимых для удовлетворения ожидаемого спроса на ИТ-услуги.

12.2 Цели процесса

Процесс Управления Мощностями направлен на постоянное предоставление необходимых ИТ-ресурсов, соответствующих текущим и будущим потребностям заказчика, в нужное время (там, где они требуются) и за приемлемую цену.

¹ Capacity manasement — более точным переводом является Управление «емкостью», т. е. управление мощностью вычислительных и телекоммуникационных средств и их потенциальными возможностями. — Прим. ред.

Поэтому для Процесса Управления Мощностями необходимо понимание как ожидаемого развития бизнеса заказчика, так и прогнозируемого технического развития. Процесс Управления Мощностями играет важную роль в определении возврата инвестиций и обосновании стоимости.

Преимущества использования процесса¹

Выгодами внедрения Процесса Управления Мощностями являются:

- снижение рисков, связанных с существующими услугами, так как осуществляется эффективное Управление Ресурсами и постоянный мониторинг производительности оборудования;
- снижение рисков, связанных с новыми услугами, так как в результате определения конфигурации технических средств для приложения (application sizing) известно влияние новых приложений на существующие системы. То же относится и к модифицированным услугам;
- снижение затрат, так как инвестиции происходят в соответствующие моменты времени, не слишком рано и не слишком поздно, что означает, что закупки не приходится делать в последнюю минуту или покупать большие мощности впрок, раньше, чем они необходимы;
- снижение угрозы срыва работы бизнес-процессов за счет тесного взаимодействия с Процессом Управления Изменениями при определении воздействия изменений на мощности ИТ и телекоммуникационных средств и предотвращении экстренных изменений из-за неправильного расчета мощностей средств;
- составление более точных прогнозов при накоплении информации Процессом Управления Мощностями, что позволяет быстрее реагировать на запросы заказчика;
- рост рациональности² работы за счет заблаговременного достижения баланса спроса и предложения;
- Управление Затратами или даже снижение затрат, связанных с мощностью средств, по причине их более рационального³ использования.

Эти преимущества приводят к улучшению взаимоотношений с заказчиками. Процесс Управления Мощностями осуществляет взаимодействие с заказчиком на ранней стадии и позволяет предвидеть его требования. Также улучшаются взаимоотношения с поставщиками. Закупка, поставка, установка и обслуживание могут планироваться более эффективно.

12.3. Процесс

Как многие процессы библиотеки ITIL, Управление Мощностями берет свое начало от эры больших ЭВМ. Из-за этого, к сожалению, некоторые считают, что Управление Мощностями необходимо только в среде больших ЭВМ. Недооценка процесса усиливается значительным снижением цен на аппаратное обеспечение в последние годы. В результате многие просто покупают аппаратные средства с избыточной мощностью, не осуществляя Управление Мощностями. Опасность заключается в том, что наибольшим источником затрат, рисков и возможных проблем в ИТ является не само аппаратное обеспечение. Другими словами, ненужное наращивание аппаратных средств создает проблемы менеджмента, которые обходятся более дорого, чем сами аппаратные средства.

Внедрение Процесса Управления Мощностями поможет предотвратить как ненужные инвестиции, так и проведение изменений мощностей случайным образом⁴, так как последний аспект может особенно отрицательно сказаться на предоставлении услуг. В настоящее время стоимость ИТ складывается не столько из вложений в мощности средств ИТ, сколько из управления ими. Например, избыточное увеличение емкости дисковой памяти влияет на резервное копирование на внешний ленточный носитель, так как поиск архивируемых файлов в сети займет больше времени. Этот пример иллюстрирует важный аспект Процесса Управления

¹ Advantages

² Efficiency.

³ Efficiently.

⁴ В данном случае это перевод словосочетания ad hoc.

Мощностями: качественное Управление Мощностями является, вероятно, наиболее важным фактором для изменения восприятия (и реального положения) ИТ-организации: не как группы, увеличивающей накладные расходы, а как поставщика услуг. При хорошем Управлении Мощностями поставщик ИТ-услуг увидит, например, что восемнадцать стратегических инициатив, намеченных в ИТ в этом году, потребуют нового решения по резервному копированию.

Понимая это, Руководитель Процесса Управления Мощностями может определить реальную стоимость этих инициатив, то есть учесть, что стоимость нового решения резервного копирования распределена по этим восемнадцати инициативам. Это будет проактивным решением. С другой стороны, при отсутствии Управления Мощностями ИТ-организация отреагирует только после того, как мощности средств резервного копирования будут исчерпаны. В этом случае заказчик будет воспринимать ИТ-расходы как накладные, а ИТ-организацию - как «выпрашивающую деньги», просто потому, что она не действовала проактивно в установлении и управлении ожиданиями заказчика и в заблаговременном планировании расходов.

Процесс Управления Мощностями направлен на предотвращение неожиданных и поспешных закупок путем лучшего использования имеющихся ресурсов, на своевременное наращивание мощности и на управление использованием текущих мощностей. Этот процесс может также помочь в координации различных компонент сервиса, что обеспечит рациональное использование инвестиций в соответствующие компоненты.

Современная ИТ-инфраструктура является чрезвычайно сложной. Это приводит к усилению зависимостей между мощностями ее компонентов. В результате становится более трудно предоставлять заказчику сервис на согласованном уровне. Поэтому профессиональная ИТ-организация должна использовать комплексный подход к Управлению Мощностями.

На рис. 12.1 показаны основные виды деятельности, выполняемые в рамках Процесса Управления Мощностями.



Рис. 12.1. Процесс Управления Мощностями (источник: OGC)

Процесс Управления Мощностями состоит из трех подпроцессов (или уровней) анализа мощностей:

- **Управление Возможностями Бизнеса** — задачей этого подпроцесса является понимание будущих потребностей пользователей. Оно может быть достигнуто за счет получения информации от заказчика, например из его стратегических планов или за счет проведения анализа тенденций. Этот подпроцесс является проактивным. Он имеет тесную взаимосвязь с процессом Управления Уровнем Сервиса при определении и ведении переговоров о сервисных соглашениях.

- **Управление Возможностями Сервиса** — задачей этого подпроцесса является определение и понимание уровня использования ИТ-услуг заказчиками (продуктов и услуг, предоставляемых заказчиком). Для заключения подходящего Соглашения об Уровне Сервиса и гарантии его выполнения необходимо знать показатели производительности и пиковой нагрузки на системы.

- **Управление Мощностями Ресурсов** — задачей этого подпроцесса является определение и понимание использования ИТ-инфраструктуры. Примерами ресурсов могут быть полоса пропускания сети, мощность средств обработки данных и емкость дисковой памяти. Для эффективного¹ Управления Ресурсами необходимо заранее определить потенциальные проблемы. Необходимо также быть в курсе тенденций развития ИТ-инфраструктуры. В рамках этого подпроцесса важным видом деятельности является активный мониторинг тенденций развития.

Так как Процесс Управления Мощностями и потребности бизнеса связаны между собой, Управление Мощностями является существенным элементом процесса планирования. Однако нельзя недооценивать и поддержку, предоставляемую им для операционных процессов². Ниже рассматриваются связи этого процесса с другими процессами Сервис-менеджмента.

Взаимоотношения с Процессом Управления Инцидентами

Управление Инцидентами информирует процесс Управления Мощностями об инцидентах, возникших из-за проблем с мощностью средств ИТ. Управление Мощностями может предоставить Управлению Инцидентами шаблоны (методики, описание шагов и действий)³ для диагностики или решения этих проблем.

Взаимоотношения с Процессом Управления Проблемами

Управление Мощностями поддерживает Процесс Управления Проблемами в его как реактивной, так и проактивной деятельности. Инструментарий Процесса Управления Мощностями, информация, накопленная в ходе его работы, знания и экспертиза могут использоваться для поддержки Процесса Управления Проблемами на различных этапах.

Взаимоотношения с Процессом Управления Изменениями

Сотрудники, участвующие в Процессе Управления Мощностями могут входить в состав Консультативного совета по изменениям⁴. Управление Мощностями может предоставлять информацию о потребности в мощностях и потенциальном воздействии изменений на предоставление услуг. Информация об изменениях является входными данными для составления Плана по мощностям⁵. Во время разработки этого плана Процесс Управления Мощностями может направлять Запросы на изменения (RFC)⁶.

¹ Effectively.

² Operational processes.

³ Scripts.

⁴ Change Advisory Board - CAB.

⁵ Capacity Plan.

⁶ Request For Change - RFC.

Взаимоотношения с Процессом Управления Релизами

Процесс Управления Мощностями поддерживает планирование распространения релизов при использовании компьютерных сетей для их тиражирования автоматическими и ручными средствами.

Взаимоотношения с Процессом Управления Конфигурациями

Между Базой Данных Мощностей¹ (CDB) и Конфигурационной Базой Данных (CMDB) существует тесная взаимосвязь. Информация, предоставляемая Процессом Управления Конфигурациями, существенно необходима для разработки эффективной базы данных мощностей.

Взаимоотношения с Процессом Управления Уровнем Услуг

Процесс Управления Мощностями дает рекомендации Процессу Управления Уровнем Услуг по вопросу реалистичности обсуждаемых Уровней Сервиса (например, скорости реакции приложения). Управление Мощностями осуществляет измерение и мониторинг производительности и предоставляет контрольную информацию для проверки исполнения согласованного Уровня Сервиса, а при необходимости и инициирует изменение Уровня Услуг и составляет необходимые отчеты.

Взаимоотношения с Процессом Управления Финансами ИТ

Управление Мощностями поддерживает составление плана инвестиций, анализ соотношения доходов и расходов² и принятие решений по инвестициям. Кроме того, этот процесс предоставляет важную информацию для выставления счетов по услугам, связанных с предоставлением мощностей, например, выделение сетевых ресурсов.

Взаимоотношения с Процессом Управления Непрерывностью ИТ-услуг

Управление Мощностями определяет минимальную мощность, необходимую для продолжения оказания услуги в случае непредвиденных обстоятельств. Мощности, необходимые для Управления Непрерывностью ИТ-сервисов должны постоянно проверяться (пересматриваться), чтобы обеспечить их соответствие ежедневным изменениям в операционной среде.

Взаимоотношения с Процессом Управления Доступностью

Процессы Управления Мощностями и Управления Доступностью тесно связаны между собой. Проблемы с производительностью и мощностью могут привести к срыву работы ИТ-услуг. В действительности заказчик может считать малую производительность работы сервиса равнозначной недоступности. Необходима эффективная координация этих двух процессов из-за их тесной взаимозависимости. В них используется большое количество одинаковых инструментальных средств и методик, таких как анализ степени влияния сбоя компонентов (Component Failure Impact Analysis - CFIA) и анализ дерева сбоев (Fault Tree Analysis - FTA).

12.4. Виды деятельности

Ниже описываются виды деятельности в рамках Процесса Управления Мощностями с разделением по каждому подпроцессу.

12.4.1. Управление Возможностями Бизнеса (Business Capacity Management)

Управление Мощностями Бизнеса включает следующие виды работ:

¹ Capacity Database - CDB.

² Cost/benefit analysis.

Разработка Плана по мощностям¹

В Плане по мощностям описываются текущие мощности ИТ-инфраструктуры и ожидаемые изменения спроса на ИТ-услуги, замена устаревших компонентов и планы технического развития. План по мощностям также определяет изменения, необходимые для предоставления услуг на согласованном в SLA уровне по приемлемой стоимости. То есть План по мощностям описывает не только ожидаемые изменения, но и связанные с ними затраты. Этот план должен составляться ежегодно и проверяться ежеквартально для подтверждения его актуальности.

В определенном смысле План по мощностям является самым важным выходным документом Процесса Управления Мощностями. В выходные данные часто включают годовой план, согласованный по срокам с бюджетом или инвестиционным планом, долгосрочный план и ежеквартальные планы с подробной информацией о запланированных изменениях мощностей. Совместно это представляет собой комплект связанных между собой планов, где уровень детализации повышается с приближением сроков планирования.

Моделирование

Моделирование является мощным инструментом Управления Мощностями, используемым для прогнозирования тенденций в инфраструктуре.

В рамках Процесса Управления Мощностями используется широкий диапазон инструментальных средств — от инструментариев оценки до средств всестороннего тестирования прототипов. Первые недороги и часто применимы в повседневной деятельности. Вторые обычно подходят только для крупномасштабных проектов внедрения.

Между этими двумя полюсами существует большое количество подходов, которые точнее оценок и дешевле крупных экспериментальных макетов. В порядке повышения их стоимости они включают в себя:

- анализ тенденции (самый дешевый способ);
- аналитическое моделирование;
- имитационное моделирование²;
- тестирование в сравнении с некоторым базовым вариантом³, также называемый бенчмаркинг (дает наиболее точную оценку).

Анализ тенденции может использоваться для получения информации о допустимой нагрузке, но не для предсказания времени реакции приложения. Аналитическое и имитационное моделирование имеют свои достоинства и недостатки. Например, имитационное моделирование может использоваться для точного предсказания производительности центрального компьютера⁴, возможно, в рамках работ по определению необходимого размера технической платформы для работы ПО⁵. Однако этот метод связан с большими затратами времени. Аналитическое математическое моделирование обычно занимает меньше времени, но получаемая на выходе информация менее надежна. Тестирование в сравнении с некоторым базовым вариантом (бенчмаркинг) означает, что создается среда с реальными условиями, например в вычислительном центре поставщика. Эта среда удовлетворяет требованиям к производительности и используется для моделирования типа «что если» или моделирования изменений. Например, таких как «что случится, если компонент приложения будет переведен на другую компьютерную систему?» или «что случится, если мы удвоим количество транзакций?».

¹ Capacity Plan.

² Simulation.

³ Baseline assessment (benchmark).

⁴ Host.

⁵ Application sizins.

Определение размера технической платформы для работы ПО¹

На этом этапе происходит определение конфигурации технических средств, необходимой для работы новых или измененных приложений, например, таких, которые находятся в стадии разработки или которые могут быть закуплены по запросу заказчика. Эти расчеты содержат информацию об ожидаемом уровне производительности, необходимых аппаратных средствах и затратах. Такой порядок действий особенно актуален на начальных стадиях разработки ПО. Ясная информация о требуемых аппаратных средствах и других ИТ-ресурсах, а также об ожидаемых затратах на начальной стадии представляет ценность для руководства. Это также помогает при разработке прототипов новых Соглашений об Уровне Услуг (SLA).

Работы по определению размеров необходимой технической платформы могут потребовать значительных усилий в крупных компаниях или в организациях со сложной ИТ-инфраструктурой. В начале в рамках Процесса Управления Мощностями происходит согласование с разработчиками Требований к Уровню Сервиса, который должен быть реализован с помощью продукта. Когда продукт достигает этапа приемо-сдаточных испытаний, выполняется проверка достижения требуемого уровня сервиса в терминах производительности центрального процессора (CPU), устройств ввода-вывода (I/O), сети, использования дисковой и оперативной памяти.

Одним из результатов этапа по определению размеров технической платформы являются показатели рабочей нагрузки. Они могут использоваться для прогнозирования необходимой мощности, например, что будет, если число пользователей возрастет на 25%. Другими показателями рабочей нагрузки являются требования по мощности во времени (пиковые нагрузки в течение суток/недели/года и перспективы будущего роста).

12.4.2. Управление Возможностями Сервисов и Управление Мощностями Ресурсов

Эти подпроцессы включают одинаковые виды деятельности, но с акцентом на различные аспекты. Управление Возможностями Сервисов обращается к предоставлению ИТ-услуг, а Управление Мощностями Ресурсов — к технологическим аспектам их предоставления. Виды деятельности показаны на рис. 12.2.

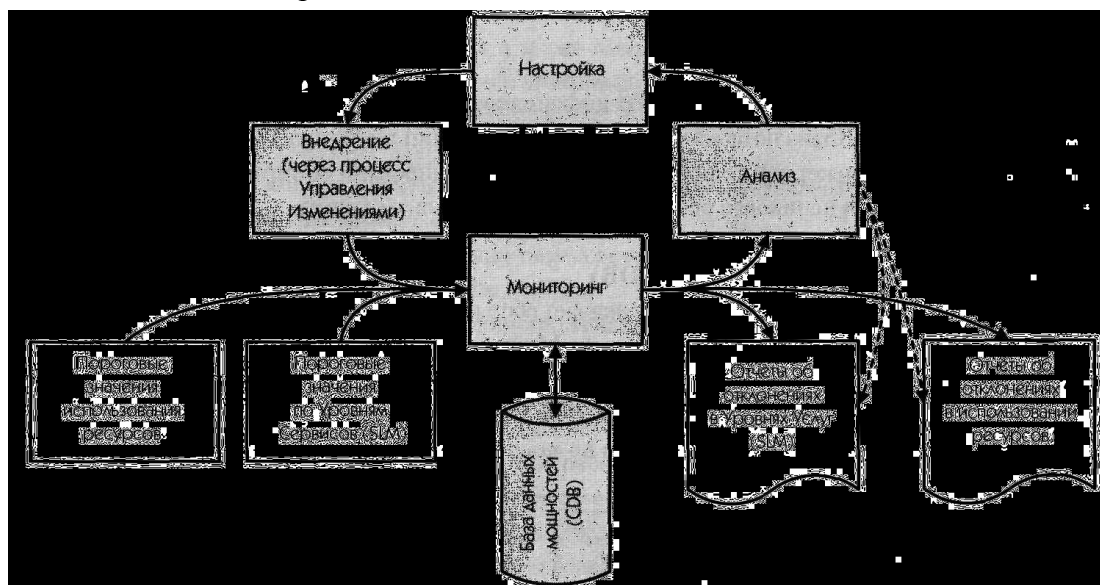


Рис. 12.2. управление Производительностью Ресурсов и Сервисов (источник: OGC)

Мониторинг

Мониторинг компонентов инфраструктуры ведется с целью гарантии выполнения согласованных Уровней Сервисов. Примерами ресурсов, в отношении которых может проводиться мониторинг, являются использование процессоров (CPU), диска, сети, числа лицензий (т. е., например, существует только десять свободных лицензий) и т. д.

¹ Application sizing.

Анализ

Данные мониторинга необходимо анализировать. Для прогнозирования будущего использования можно применять анализ тенденций. Результаты анализа могут привести к началу работ по повышению рациональности использования или к приобретению дополнительных ИТ-компонентов. Анализ деятельности требует глубокого знания всей инфраструктуры и бизнес-процессов компании.

Настройка

Настройка выполняется с целью оптимизации систем для текущей или ожидаемой рабочей нагрузки на основе результатов анализа и интерпретации данных мониторинга.

Внедрение

Целью внедрения является ввод измененной или новой мощности. Если это связано с изменением, то внедрение вовлекает Процесс Управления Изменениями.

Управление Спросом

Управление Спросом нацелено на вопросы потребления ИТ-мощностей. Управление Спросом занимается изучением влияния различных факторов на спрос. Простой пример: пользователь запускает плохо написанный SQL-отчет в середине дня, преграждая другим пользователям доступ к базе данных и создавая непомерный трафик. Руководитель Процесса Управления Мощностями предлагает запускать задание по составлению отчета ночью, так, чтобы пользователь получал результат на своем столе утром. Проведем различие между Управлением Краткосрочным и Долгосрочным Спросом:

- **Управление Краткосрочным Спросом** — в случае, если в ближайшем будущем есть угроза повторяющейся нехватки мощностей ИТ-средств и если доступ к дополнительным мощностям затруднен;
- **Управление Долгосрочным Спросом** — если не удастся обосновать стоимость модернизации, хотя в определенные периоды времени (например, между 10:00 и 12:00) может возникать недостаток мощности.

Управление Спросом предоставляет важную информацию для составления, мониторинга и, возможно, корректировки как Плана по мощностям, так и Соглашений об Уровнях Сервиса. Управление Спросом может также использовать дифференцированную тарификацию (т. е. различные тарифы в пиковое и не пиковое время) для воздействия на заказчика.

Заполнение Базы Данных Мощностей (CDB)

Создание и заполнение базы данных CDB означает сбор и обновление технической, бизнес-и любой другой информации, относящейся к Управлению Мощностями. Может быть, нереально хранить всю информацию по мощностям в одной физической базе данных. Руководители по сетевым и компьютерным системам могут использовать свои собственные методы. Часто база данных CDB содержит ссылки на различные источники информации по мощностям ИТ-систем.

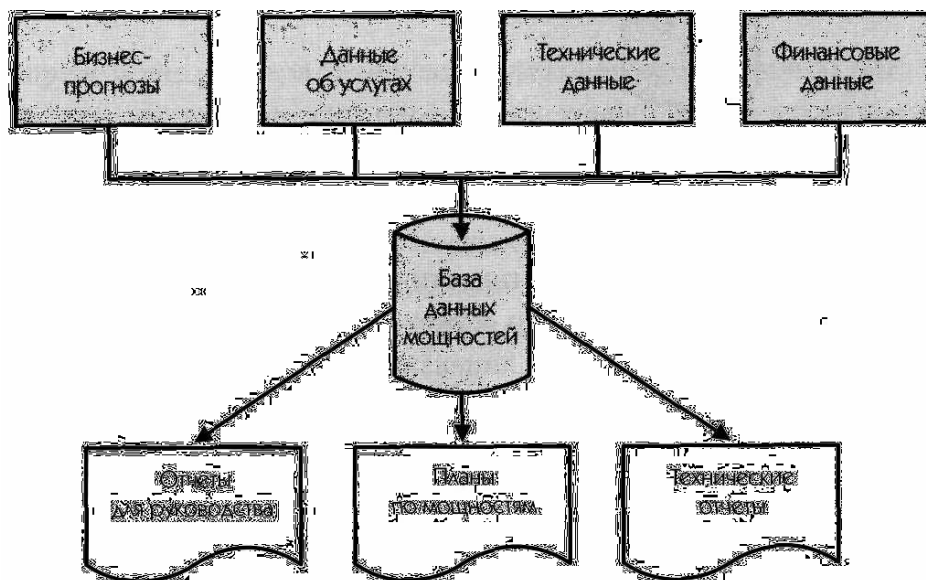


Рис. 12.3. Источники информации для базы данных CDB

12.5. Контроль процесса

Процесс Управления Мощностями наиболее эффективен в случае, если он тесно связан с другими процессами планирования, такими как Управление Доступностью, и с деятельностью по разработке приложений. Такая взаимосвязь способствует использованию проактивного подхода в работе Процесса Управления Мощностями.

12.5.1. Отчеты для руководства

Представляемые процессом отчеты для руководства содержат, с одной стороны, информацию об Управлении Процессом в терминах показателей Плана по мощностям, ресурсов, используемых для реализации процесса, и деятельности по совершенствованию процесса; а с другой стороны отчеты об отклонениях по таким вопросам как:

- расхождения между фактическим и плановым использованием мощностей;
- тенденции в расхождениях;
- воздействие на Уровни Сервиса;
- ожидаемое увеличение/уменьшение использования мощностей в краткосрочной и долгосрочной перспективе;
- пороговые значения, при достижении которых потребуется приобретение дополнительных мощностей.

12.5.2. Критические факторы успеха и Ключевые Показатели Эффективности (KPI)

Управление Мощностями зависит от следующих критических факторов успеха:

- точной оценки бизнес-планов и ожиданий заказчиков;
- понимания ИТ-стратегии и планирования, а также точности планирования;
- оценки ведущихся технических разработок в компании;
- взаимодействия с другими процессами.

Следующие параметры могут служить Ключевыми Показателями Эффективности (KPI) работы Процесса Управления Мощностями:

- Предсказуемость потребностей заказчика: определение изменений рабочей нагрузки и тенденций, а также точность Плана по мощностям.

- **Технология:** различные варианты измерения производительности ИТ-сервисов, темпы внедрения новых технологий и возможность постоянно выполнять Соглашения об Уровне Услуг (SLA) даже при использовании старых технологических средств.
- **Затраты:** уменьшение числа срочных закупок, сокращение ненужных или дорогих избыточных мощностей и составление планов инвестиций на ранней стадии.
- **Операционная деятельность ИТ¹:** уменьшение количества инцидентов из-за проблем с производительностью, возможность удовлетворить спрос заказчика в любое время и степень серьезности в отношении компании к Процессу Управления Мощностями.

12.5.3. Функции и роли

Роль Руководителя Процессы Управления Мощностями заключается в руководстве процессом и в обеспечении разработки и поддержания Плана по мощностям, а также в гарантии актуальности базы данных мощностей (CDB).

Менеджеры систем, сетей и приложений также играют важную роль в Процессы Управления Мощностями. Они не только являются ответственными за оптимизацию производительности, от них также ожидается использование их профессиональных знаний для преобразования потребностей бизнеса в профили² загрузки систем и определения на их основе необходимых мощностей ИТ-средств.

12.6. Проблемы и затраты

12.6.1. Проблемы

Потенциальные проблемы Процессы Управления Мощностями могут быть следующими:

- **Нереалистичные ожидания** — разработчики³, руководители и заказчики часто имеют нереалистичные ожидания из-за недостаточного понимания технических возможностей приложений, компьютерных систем и сетей. Одной из задач Процессы Управления Мощностями является направление этих ожиданий, например, путем осведомления разработчиков о воздействии их разработок (например, базы данных) на мощности ИТ-средств и их производительность. Эффект от работы Процессы Управления Мощностями также может переоцениваться, особенно в отношении настройки системы и составления графика рабочей нагрузки. Если работа системы требует значительной настройки, то, скорее всего, причина в недостатках дизайна приложения или базы данных. В целом, настройка не может быть использована для достижения более высокого уровня производительности, чем тот, на который система была рассчитана изначально. Большинство крупных ИТ-систем имеют алгоритмы планирования загрузки, которые обычно более эффективны, чем вовлечение системных менеджеров. И конечно, существуют и затраты, связанные с настройкой: для высокооплачиваемого инженера не имеет смысла тратить недели на достижение 3%-го улучшения характеристик, если расширение памяти за 100 долларов даст улучшение на 10%. Еще более дорого обойдется Управление Системами, которые не являются «простыми, как дважды два». Чрезмерное «дергание» параметров на различных блоках, приложениях или базах данных может повлечь непреднамеренные последствия и увеличит задержку всех процессов сервис-менеджмента, а также обслуживание и поиск неисправностей.

- **Недостаток соответствующей информации** — часто бывает трудно получить необходимую информацию, например, для Плана по мощностям. Могут возникнуть затруднения в получении достоверной информации об ожидаемой рабочей нагрузке, так как планы заказчика неизвестны или почти неизвестны, в особенности в деталях. Это также вызывает трудности у заказчика, так как жизненный цикл продукта становится все короче. Единственное решение — это делать наилучшие возможные оценки и периодически обновлять их при получении большей информации.

¹ Operations.

² Profiles.

³ Desisners.

- **Информация от поставщика** — при отсутствии информации о предыстории вопроса (например, когда закупается новая система), Управление Мощностями становится зависимым от информации, предоставляемой поставщиками. Поставщики обычно используют результаты тестов¹ для предоставления информации об их системах, но из-за больших различий в методах тестирования часто бывает трудно сопоставить информацию, и она может ввести в заблуждение о действительной производительности системы.

- **Внедрение в комплексных ИТ-средах** — внедрение в сложных распределенных средах является трудной задачей, так как значительное количество технических интерфейсов создает большое число взаимозависимостей параметров производительности.

- **Определение подходящего уровня мониторинга** — инструменты для мониторинга часто имеют много опций и могут провоцировать на чрезмерно подробные исследования. При покупке и использовании этих инструментов необходимо заранее решить, на каком уровне детализации должен проводиться мониторинг.

Эти проблемы являются актуальными для Управления Мощностями компьютерных систем, а также сетей, больших принтерных центров и телефонных АТС-систем². Это может вызвать еще больше затруднений, если за эти области отвечают несколько подразделений, что может привести к конфликтам в ответственности за Управление Мощностями.

12.6.2. Затраты

Затраты на ввод в действие Управления Мощностями должны быть определены при подготовке внедрения процесса. Эти затраты можно разделить на следующие группы:

- закупка аппаратных и программных средств, таких как инструменты мониторинга, база данных мощностей (CDB), инструменты моделирования для имитационного моделирования и статистического анализа и инструменты генерации отчетов;
- затраты на Управление Проектом по внедрению процесса;
- затраты на персонал, обучение и поддержку;
- помещение и т. д.

После запуска процесса остаются текущие расходы на персонал, контракты на обслуживание и т. д.

¹ Benchmarks.

² PABX.

Глава 13

Управление Непрерывностью ИТ-сервисов

13.1. Введение

Многие руководители считают Процесс Управления Непрерывностью ИТ-сервисов (IT Service Continuity Management — ITSCM) роскошью, на которую у них нет средств. Однако, как показывает статистика, чрезвычайные ситуации стали часто встречающимся явлением.

Чрезвычайная ситуация (бедствие, катастрофа) — это событие, которое оказывает такое негативное воздействие на функционирование сервиса или системы, что требуются значительные усилия для восстановления изначального Уровня Производительности.

Как следует из данного определения, чрезвычайная ситуация намного серьезнее инцидента. Чрезвычайная ситуация — это приостановка бизнеса. Это означает, что весь бизнес или его часть будет находиться «вне бизнеса» после возникновения чрезвычайной ситуации. Известны такие примеры чрезвычайных ситуаций, как пожары, удары молнии, наводнения, кражи, вандализм и акты насилия, широкомасштабное нарушение электроснабжения и сбои в работе аппаратного обеспечения. Атаки террористов, например, нападение на Всемирный торговый центр в Нью-Йорке, становятся реальностью. Чрезвычайные ситуации возможны также и в Интернете, например, отказ сервиса (DoS)¹ может разрушить связь внутри всей организации. Некоторые организации могли бы предотвратить серьезные проблемы, если бы в свое время разработали План обеспечения непрерывности бизнеса. Бизнес все больше и больше зависит от ИТ-услуг, а это означает, что последствия потери сервиса становятся все более ощутимыми и все менее допустимыми. Фактически, сейчас во многих организациях ведение бизнеса эквивалентно использованию информационных технологий (ИТ), и без них бизнес едва ли будет существовать. Поэтому необходимо решать, как защитить непрерывность бизнеса. Со времени опубликования модуля Планирование на случай чрезвычайных обстоятельств (Contingency Planning Module) ассоциацией ССТА многое изменилось в области информационных технологий и в том, как они используются в организациях. Ранее это планирование касалось только ИТ. В настоящий момент информационные технологии уже значительно интегрированы во многие аспекты бизнеса. Если раньше традиционный процесс планирования непрерывности работы и восстановления функционирования в основном носил реактивный характер (что делать в случае возникновения чрезвычайной ситуации), то теперь Процесс Управления Непрерывностью ИТ-сервисов выполняет превентивную роль, т. е. работает над предотвращением катастроф.

13.2. Цель процесса

Цель Процесса Управления Непрерывностью ИТ-сервисов — оказывать поддержку Процессу Управления Непрерывностью Бизнеса (Business Continuity Management — BCM). Такая поддержка означает, что необходимая инфраструктура и ИТ-услуги, включая службу поддержки и службу Service Desk, могут быть восстановлены за заданный период времени после возникновения чрезвычайной ситуации. У данного процесса может быть и ряд других целей. Поскольку процесс ITSCM является составной частью Процесса Управления Непрерывностью Бизнеса, сфера действия Процесса Управления Непрерывностью ИТ-сервисов (ITSCM) должна определяться, исходя из целей бизнеса. В результате при оценке рисков можно потом определить, попадают ли они в сферу действия данного процесса.

Преимущества использования процесса²

Поскольку бизнес во все большей степени зависит от ИТ-услуг, определить, во что может обойтись недостаточное планирование непрерывности предоставления ИТ-услуг и какие преимущества даст должное планирование этих вопросов, можно только с помощью анализа рисков. После того, как определен возможный риск для бизнеса, а не только для ИТ-сервиса,

¹ Denial of Service - DoS.

² Benefits.

можно выделять средства для принятия превентивных мер и мер по борьбе с чрезвычайными ситуациями, например, разработка Плана восстановления после катастрофы.

Если чрезвычайная ситуация все же произошла, то использование процесса ITSCM даст бизнесу следующие преимущества:

- возможность управлять восстановлением своих систем;
- уменьшить простои в работе;
- свести к минимуму перерывы в ведении бизнеса.

13.3. Процесс

Процесс Управления Непрерывностью ИТ-сервисов отвечает за:

- оценку воздействия нарушений в работе ИТ-сервисов после возникновения чрезвычайной ситуации;
- определение критичных для бизнеса сервисов, которые требуют дополнительных превентивных мер;
- определение периода времени, в течение которого сервис должен быть восстановлен;
- принятие мер по предотвращению, обнаружению, подготовке к чрезвычайным ситуациям или по уменьшению степени их воздействия;
- определение общего подхода к восстановлению услуг;
- разработку, тестирование и поддержку плана восстановления с достаточным Уровнем Детализации, который поможет пережить чрезвычайную ситуацию и восстановить нормальную работу за заданный период времени.

Поскольку наблюдается все большее взаимопроникновение бизнес-операций и информационных технологий, то эти две области вместе описываются в рамках ITIL:

- Процесс Управления Непрерывностью Бизнеса (Business Continuity Management — BCM) обеспечивает анализ и Управление Рисками, что позволяет организации во все времена гарантировать сохранение минимально требуемых производственных мощностей и Уровня Сервисов. Процесс BCM помогает уменьшить степень риска до приемлемого уровня и разработать Планы восстановления бизнес-деятельности на случай, если она пострадает во время чрезвычайной ситуации.
- Процесс Управления Непрерывностью ИТ-сервисов (ITSCM) — это процесс, предназначенный для противодействия на случай чрезвычайных обстоятельств, затрагивающих ИТ-услуги, и восстановления сервисов, необходимых для возобновления бизнес-операций.

Процесс Управления Непрерывностью ИТ-сервисов является частью общего процесса Управления Непрерывностью Бизнеса, и он зависит от информации, которую предоставляет процесс BCM. Доступность ИТ-сервисов обеспечивается благодаря сочетанию мер по уменьшению степени риска (например, использование высоконадежных систем) и способов восстановления (например, запасные и параллельно работающие системы). Для успешной реализации процесса требуются поддержка со стороны всей организации, твердое намерение руководства реализовать данный процесс и участие всего персонала.

Процесс Управления Непрерывностью ИТ-сервисов взаимодействует со всеми другими процессами ИТ Сервис-менеджмента, особенно с такими как:

- **Управление Уровнем Сервиса:** предоставляет информацию об обязательствах по предоставлению ИТ-услуг.
- **Управление Доступностью:** поддерживает процесс ITSCM в части разработки и внедрения превентивных мер.
- **Управление Конфигурациями:** определяет базисные конфигурации и элементы ИТ-инфраструктуры, информация о которых используется при восстановлении после чрезвычайной ситуации.

- **Управление Возможностями:** гарантирует поддержку требований бизнеса соответствующими ИТ-ресурсами.

- **Управление Изменениями:** обеспечивает правильность и актуальность всех планов в рамках процесса ITSCM благодаря вовлечению ITSCM в работу над всеми изменениями, которые могут повлиять на превентивные меры и Планы восстановления.

13.4. Виды деятельности

На рис 13.1 показаны виды работ, выполняемые в рамках процесса ITSCM. Цифры обозначают подразделы раздела 13.4, в которых описывается тот или иной вид деятельности.

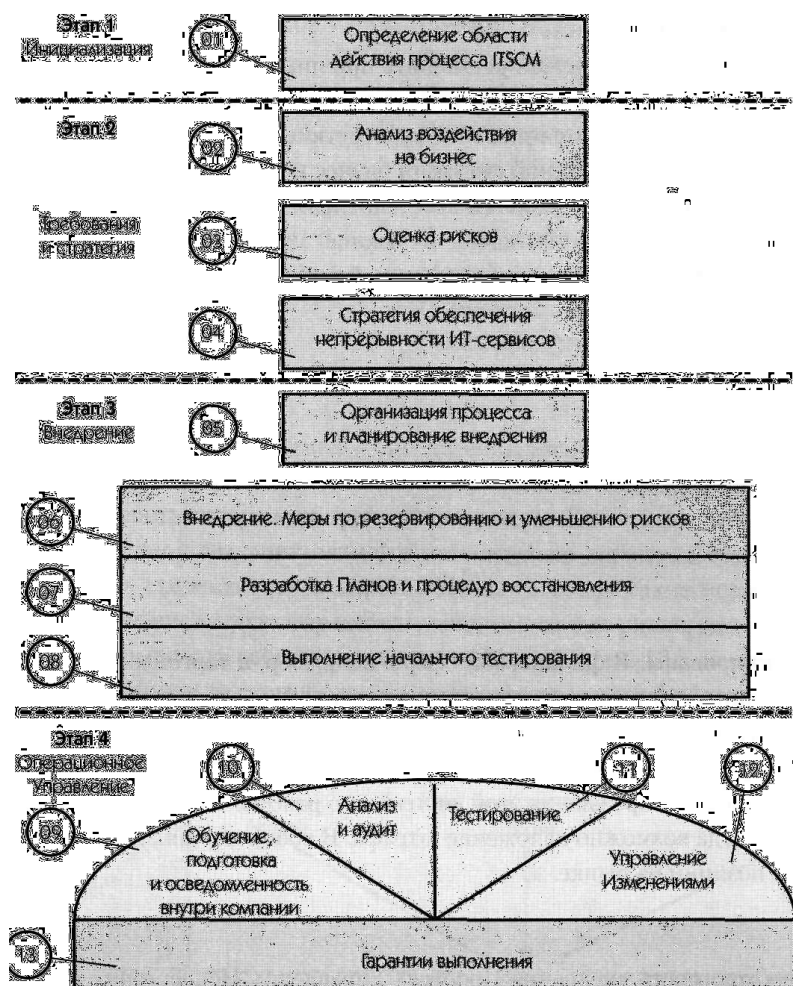


Рис. 13.1. Модель Процесса Управления Непрерывностью ИТ-сервисов (на основе модели OGC)

13.4.1. Определение охвата (области действия)¹ Процесса Управления Непрерывностью ИТ-сервисов

При инициализации процесса ITSCM необходимо рассмотрение всей организации в целом и выполнение следующих действий:

- **Определение политики** — определение политики организации в отношении Управления Непрерывностью ИТ-сервисов следует осуществить по возможности быстрее и довести ее до сведения каждого сотрудника организации, чтобы все знали о необходимости процесса ITSCM. Руководство должно продемонстрировать свое твердое намерение реализовать данный процесс.

- **Определение области действия процесса и других важных для процесса областей** — при выборе подхода к оценке риска и Анализу воздействия на бизнес (Business Impact Analysis) и

¹ Scope

методов их выполнения используются страховые требования, стандарты качества, такие как серия ISO-9000, стандарты Управления Безопасностью, например, BS7799 и общие принципы определения политики в области бизнеса. На этом этапе также определяются соответствующая структура менеджмента и процессов на случай чрезвычайной ситуации.

- **Выделение ресурсов** — развертывание ИТ-среды на случай чрезвычайных обстоятельств потребует значительных затрат на персонал и ресурсы. Должно быть проведено обучение персонала для подготовки к выполнению второго этапа процесса ITSCM (Требования и стратегия).

- **Подготовка проектной организации** — рекомендуется использовать формальные методы Управления Проектом, такие как PRINCE 2, совместно с программным обеспечением, предназначенным для целей планирования.

13.4.2. Анализ воздействия на бизнес¹

Перед проведением анализа ИТ-услуг рекомендуется установить причины, почему компании необходимо включать Процесс Управления Непрерывностью ИТ-сервисов в общий Процесс Управления Непрерывностью Бизнеса, и определить потенциальное воздействие серьезных сбоев услуг. В некоторых случаях при возникновении чрезвычайной ситуации бизнес некоторое время еще может функционировать, и тогда основное внимание уделяется восстановлению услуг, в других случаях бизнес не может работать без ИТ-услуг, поэтому основное внимание уделяется предотвращению чрезвычайных ситуаций. В большинстве случаев необходимо найти баланс между этими двумя крайностями.

Среди возможных причин внедрения этого процесса могут быть следующие:

- защита бизнес-процессов;
- быстрое восстановление сервиса;
- необходимость выдержать конкуренцию;
- сохранение позиций на рынке;
- сохранение прибыльности;
- защита репутации компании.

Эти причины могут быть комбинированы. В финансовой сфере, например, в торговле валютными средствами, отсутствие информации о рынке ведет к приостановке торговли (основного бизнес-процесса), что означает потерю денег. Более того, если существует государственное требование регистрировать все валютные операции с использованием специализированной системы, то можно продолжать ведение бизнеса даже в случае повреждения этой системы, но рано или поздно это требование все равно будет нарушено, и тогда возможно наложение штрафа. В обоих случаях компания может потерять заказчиков и свои позиции на рынке.

Анализ сервисов

После того, как определена необходимость внедрения Процесса Управления Непрерывностью ИТ-сервисов, следует провести анализ ИТ-услуг, необходимых для бизнеса (например, информационные системы, офисные приложения, бухгалтерские приложения, электронная почта и т. д.), которые должны быть доступны в соответствии Соглашениям об Уровне Сервиса. Для некоторых услуг невысокой значимости могут быть достигнуты договоренности о предоставлении экстренного сервиса с ограниченными возможностями и доступностью. Уровни Сервиса во время восстановления могут быть изменены только по договоренности с заказчиком. Для критически важных услуг необходимо найти компромисс между превентивными мерами и способами восстановления.

¹ Business Impact Analysis

Инфраструктура

После анализа сервисов выполняется оценка зависимостей между сервисами и ИТ-ресурсами. Информация из Процесса Управления Доступностью используется для анализа степени критичности ИТ-ресурсов для поддержки описанных ранее ИТ-услуг. Процесс Управления Возможностями предоставляет информацию о необходимых мощностях, а также помогает определить, на какое время эти услуги могут быть приостановлены с момента сбоя сервиса до его восстановления. В последствии такая информация может быть использована для определения способов восстановления по каждой услуге.

13.4.3. Оценка рисков

Официальная статистика по чрезвычайным ситуации отсутствует, но во всем мире известны такие катастрофы, как:

Отравление газом	Токийское метро, Япония (март 1995)
Отключение электроэнергии	Окланд, Новая Зеландия (декабрь 1997)
Землетрясения	Лос-Анджелес, США (январь 1994) Кобе, Япония (январь 1995)
Атаки террористов	Всемирный торговый центр, Нью-Йорк, США (февраль 1993) Бишопсгейт, Лондон, Англия (апрель 1993) Оклахома-сити, Оклахома, США (апрель 1995) Доклэндс, Лондон, Англия (февраль 1996) Манчестер, Англия (июнь 1996) Всемирный торговый центр, Нью-Йорк, США (сентябрь 2001)
Наводнения	Бангладеш (июль 1996) Пакистан (август 1996)

Анализ рисков способен помочь в определении рисков, угрожающих бизнесу. Такой анализ дает ценную информацию руководству, т. к. он позволяет выявить вероятные угрозы и виды уязвимости и определить соответствующие превентивные меры. Поскольку поддержка Плана восстановления после чрезвычайной ситуации является относительно дорогим мероприятием, то сначала можно воспользоваться превентивными мерами. После того, как такие меры предприняты против наиболее серьезных рисков, следует определить, остались ли еще риски, для которых необходим План обеспечения непрерывности работы (Contingency Plan). На рис. 13.2 показаны связи между Анализом рисков и Управлением Рисками; они основываются на методе Анализа и Управления Рисками, разработанного ассоциацией CCTA (CCTA Risk Analysis and Management Method — CRAMM).

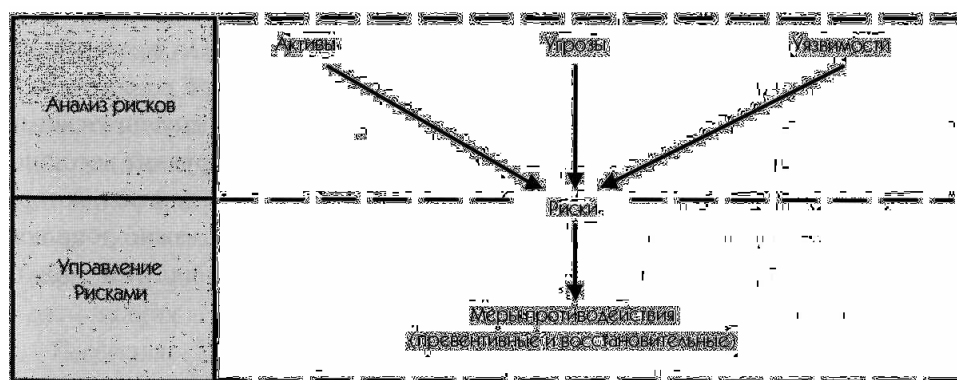


Рис 13.2. Метод оценки рисков ассоциации CCTA (источник: OGC)

Данная модель позволяет поддерживать эффективное планирование на случай чрезвычайных обстоятельств путем реализации поэтапного подхода.

Анализ рисков

- Во-первых, должны быть определены вовлеченные компоненты (активы), такие как здания, системы, данные и т. д. Эффективная идентификация активов требует определения владельцев и назначения активов.

- Следующий этап — анализ угроз и зависимостей, а также оценка вероятности возникновения чрезвычайной ситуации (высокая, средняя, низкая), например, комбинация ненадежной системы энергоснабжения и района с большим количеством бурь и гроз.

- Далее — идентификация и классификация (высокая, средняя, низкая) уязвимостей. Молнеотвод может дать некоторую защиту от ударов молний, но они все же могут серьезно повлиять на работу сети и систем.

- И последний этап — оценка угроз и уязвимостей в контексте ИТ-компонентов для получения оценки риска.

При оценке риска следует учитывать область действия¹ процесса; фактически такая оценка является частью начала внедрения Процесса Управления Непрерывностью ИТ-сервисов (этап 1). Например, незначительные проблемы можно решить с помощью мер, принимаемых Процессом Управления Доступностью, в то время как другие риски для бизнеса могут выходить за сферу действия процесса ITSCM.

13.4.4. Стратегия обеспечения непрерывности ИТ-сервисов

Многие направления бизнеса стараются найти равновесие между сокращением степени риска и планированием работ по восстановлению. Следует понимать разницу между такими понятиями, как сокращение риска, работы по восстановлению бизнес-деятельности и способы восстановления ИХ. Ниже обсуждается связь между сокращением степени риска (предотвращение) и планированием восстановления (способы восстановления).

Угрозы никогда нельзя устранить полностью. Например, пожар в соседнем здании может повредить ваше здание. Уменьшение одного вида риска может вызвать повышение другого. Например, аутсорсинг может привести к повышению рисков в области безопасности.

Превентивные меры

Превентивные меры можно принимать на основе анализа рисков при тщательном учете затрат и рисков. Такие меры могут помочь в уменьшении вероятности непредвиденных обстоятельств или степени их воздействия, и тем самым сократить сферу действия Плана восстановления. Превентивные меры действенны против пыли, чрезвычайно высоких или низких температур, пожаров, утечек воды, прекращения энергоснабжения и воровства. Остальные виды рисков будут учтены в Плане восстановления.

Метод «Неприступной крепости»² является самой дорогой превентивной мерой. Он позволяет устранить большинство видов уязвимости, например, путем строительства бункера с собственным энерго- и водоснабжением. Однако такой подход может привести к появлению других уязвимых мест, например, риску сбоя сети или появлению пробок на дорогах, что только затруднит восстановление. Подход «Неприступной крепости» пригоден для крупных вычислительных центров, которые слишком сложны для разработки для них Плана восстановления. В наше время важно дополнять данный подход возможностью быстрого реагирования³, т. е. возможностью направляться туда, где есть проблема, и быстро ее решать, пока она не вышла из-под контроля.

¹ Scope.

² Stronghold/Fortress approach.

³ Skirmish capability.

Выбор способов восстановления¹

Если остались еще виды рисков, которые не удалось устранить с помощью превентивных мер, тогда для них производится планирование восстановления. Способы восстановления должны включать в себя:

- Персонал и размещение — помещение, мебель, транспорт, способ перемещения и т. д.
- ИТ-системы и сети — способы восстановления будут обсуждаться ниже.
- Вспомогательные службы — электро- и водоснабжение, телефон, почта и курьерская связь.
- Архивы — дела, документы, архив на бумажных носителях и справочные материалы.
- Услуги сторонних организаций — таких, как поставщиков услуг электронной почты и Интернета.

Существует несколько способов для быстрого восстановления ИТ-услуг:

- **Ничего не делать** — лишь немногие бизнес-организации могут себе это позволить. Это больше напоминает стремление уйти от проблем, устранившись от решения. Подразделения, которые думают, что могут обойтись без средств восстановления ИТ-сервиса, создают о себе впечатление, как о структурах, ничего не значащих для целей бизнеса, которые могут не потребоваться в случае чрезвычайной ситуации. Тем не менее для каждого ИТ-сервиса должна быть рассмотрена такая возможность.

- **Возврат к ручной (на основе бумажных носителей) системе** — этот способ обычно не подходит для услуг, критически важных для бизнеса, поскольку трудно найти достаточное количество персонала, имеющего опыт работы с традиционными системами. Более того, бумажные системы, существовавшие в прошлом, теперь могут уже не существовать. Тем не менее такие системы можно использовать для менее важных, второстепенных услуг. Большинство планов восстановления включают в себя процедуры резервного копирования на бумажные носители. Например, способом восстановления для терминала кредитных карт может быть использование бумажных оттисков (слипов) с кредитных карт.

- **Взаимные соглашения** — этот способ можно использовать в том случае, когда две организации используют одинаковое аппаратное обеспечение и между ними существует договоренность о предоставлении друг другу необходимых устройств в случае возникновения чрезвычайных обстоятельств. Для данного способа две бизнес-структуры должны заключить соглашение и координировать все изменения, с тем чтобы сохранить взаимозаменяемость двух сред. Процесс Управления Возможностями должен следить за тем, чтобы зарезервированные возможности не использовались для других целей или чтобы их можно было быстро освободить. В настоящее время этот способ не очень привлекателен из-за роста использования онлайн-систем, таких как сети банкоматов (АТМ) и онлайн-банковские системы для клиентов, т. е. эти системы должны быть доступны круглосуточно в течение всего времени.

- **Поэтапное восстановление («холодный» резервный центр²)** — этот способ можно использовать в тех сферах бизнеса, где можно обойтись без ИТ-услуг в течение определенного периода времени, например, 72-х часов. При использовании данного способа заказчику предоставляется свободный компьютерный зал на заранее оговоренной территории, *стационарный центр³* или мобильная компьютерная комната, доставляемая на место расположения компании, — *мобильный центр⁴*. Такой компьютерный центр должен быть снабжен электропитанием, кондиционером, сетевыми коммуникациями и телефонной связью. Данный способ может быть предоставлен по договору с внешним поставщиком. Кроме того, необходимо отдельное соглашение с поставщиком, гарантирующее быструю доставку ИТ-компонент. Общее преимущество такого подхода состоит в том, что эти средства восстановления

¹ Recovery options.

² Cold stand-by.

³ Fixed facility.

⁴ Mobile facility.

доступны всегда. Кроме того, для стационарного и мобильного компьютерного центра преимущества и недостатки различаются и зависят от таких аспектов, как:

- *Расстояние до центра* — обычно существует ограниченное количество поставщиков, предоставляющих услуги стационарного центра, и он может находиться на некотором расстоянии от заказчика. Этот недостаток может быть компенсирован использованием мобильной станции.

- *Время* — стационарные залы доступны лишь на определенное время.

- *Задержка* — в любом случае доставка необходимого компьютерного оборудования занимает определенное время.

- *Сеть* — часто возникают трудности с предоставлением нужных телекоммуникационных средств. Оборудование передвижной станции можно подсоединить к сети в основном используемом здании.

- **Промежуточное восстановление («теплый» резерв¹)** — данный способ обеспечивает доступ к аналогичной операционной среде, в которой можно восстановить обычное предоставление услуг в течение короткого промежутка времени (от 24 до 72 часов). Существует три варианта этого способа:

- *Внутренний* (совместное устранение неисправности): применим в тех случаях, когда бизнес располагается на нескольких площадках или имеет выделенную среду тестирования, которую можно использовать в качестве рабочей среды. Данный способ обеспечивает полное восстановление при минимальных затратах времени на переключение. В организациях с несколькими распределенными системами часто используется один из вариантов этого подхода, когда на каждой системе резервируется часть требуемых мощностей. Мониторинг таких свободных мощностей осуществляется Процессом Управления Мощностями (аналогично варианту использования взаимных соглашений — см. выше).

- *Внешний*: некоторые поставщики услуг предлагают этот способ как коммерческую услугу. При этом затраты распределяются между несколькими заказчиками. Расходы по данному варианту зависят от того, какое программное и аппаратное обеспечение потребуется, на какой период времени будут предоставляться средства (например, на 16 недель). Часто этот способ помогает сохранить работоспособность на период времени, в течение которого активируется «холодный» резервный центр. Данный вариант способа промежуточного восстановления относительно дорогостоящий и предоставленный центр, скорее всего, будет находиться на некотором удалении от основной территории.

- *Мобильный*: в данном варианте готовая к работе инфраструктура размещается в трейлере, который используется как компьютерный зал и оборудован устройствами контроля за окружающей средой, такими как кондиционеры. У ИТ-организации должно быть место для парковки такого трейлера. В специально выделенных пунктах на некотором расстоянии от основного здания должны быть предусмотрены источники электропитания, телекоммуникационные каналы и хранилище данных. Преимуществами такой версии являются быстрое время реагирования и близость к месту расположения компании. Данный способ доступен только для ограниченного числа технических платформ. Некоторые крупные поставщики оборудования предлагают несколько трейлеров со стандартными конфигурациями аппаратного обеспечения. В согласованный момент времени, например, раз в год, такой трейлер направляется к месту расположения бизнеса для проверки Плана восстановления. Кроме того, такая процедура позволяет произвести тестирование перехода² на новую версию операционной системы.

- **Немедленное восстановление («горячий» старт, «горячее» восстановление³)** - данный способ обеспечивает немедленное или очень быстрое восстановление работы менее чем за 24 часа путем предоставления идентичной рабочей среды и зеркального отображения данных, а

¹ Warm stand-by.

² Upgrade.

³ Hot start, hot stand-by.

возможно, и рабочих процессов. Последний вариант обычно разрабатывается при тесном взаимодействии с Процессом Управления Доступностью.

- **Комбинации способов** — часто План на случай чрезвычайных обстоятельств¹ включает в себя более дорогой способ восстановления, который используется до активизации более дешевого варианта. Например, трейлер, оборудованный как передвижной вычислительный центр (мобильный «горячий» старт), может служить временным решением до тех пор, пока не придет мобильный центр и не будут доставлены новые главные сервера² (передвижной «холодный» старт). Нормальная работа будет возобновлена после восстановления здания и установки в нем новых главных компьютеров.

13.4.5. Организация процесса и планирование внедрения

После того, как определена стратегия бизнеса и сделан выбор одного из перечисленных способов восстановления, необходимо переходить к реализации Процесса Управления Непрерывностью ИТ-сервисов и разработки детальных планов для использования выбранных средств восстановления. Реализацией процесса ITSCM должна заниматься специальная группа. Ее организация может включать в себя назначение руководителя (Руководитель на случай кризисной ситуации³), координацию работ и формирование восстановительных команд каждого сервиса.

На самом высоком уровне должен быть разработан общий план, охватывающий следующие вопросы:

- План экстренного реагирования;
- План оценки повреждений;
- План восстановления работы;
- План работы с важными данными (что делать с данными, включая записи на бумажных носителях);
- План руководства на случай кризисной ситуации и связь с общественностью (PR).

Все эти планы используются для оценки экстренных ситуаций и определения мер реагирования на них. После этого можно принимать решение об инициировании процесса восстановления бизнеса, при котором начинают действовать планы следующего уровня, включающие:

- План размещения и оказания услуг;
- План по вычислительным системам и локальным сетям;
- План по телекоммуникациям (доступ и каналы связи);
- План обеспечения безопасности (целостность данных и сетей);
- План по персоналу;
- Финансовые и административные планы.

13.4.6. Применение превентивных мер и способов восстановления

Этот этап заключается в практическом воплощении определенных ранее превентивных мер и способов восстановления. Превентивные меры по уменьшению степени воздействия предпринимаются совместно с деятельностью в рамках Процесса Управления Доступностью и могут включать:

- Использование бесперебойных источников питания и резервных источников электропитания;

¹ Contingency plan.

² Host computers.

³ Crisis Manager.

- Использование отказоустойчивых систем¹;
- Использование удаленных систем хранения данных и RAID-массивов и т. д.

Также должен быть объявлен стартовый срок для активизации резервных соглашений, включающих персонал, здания и телекоммуникации. Даже еще во время действия непредвиденных обстоятельств уже можно начинать работы по восстановлению нормальной деятельности и заказу новых ИТ-компонентов. Рамочные неактивированные («дремлющие») договоры на такой случай могут быть заключены с поставщиками заранее. В этом случае уже будут подписаны заказы на поставку компонентов по согласованной ранее цене. В случае чрезвычайной ситуации поставщик будет исполнять заказ без необходимости обсуждения его цены. Такие неактивированные («дремлющие») договоры следует пересматривать каждый год, т. к. цены и модели технических средств могут изменяться. При корректировке договоров следует учитывать базисные конфигурации, зарегистрированные в рамках Процесса Управления Конфигурациями. При подготовке резервных соглашений могут осуществляться следующие виды деятельности:

- ведение переговоров со сторонними организациями по вопросам удаленных средств восстановления;
- поддержка и оснащение средств восстановления;
- закупка и установка резервного аппаратного обеспечения (неактивированные договоры);
- управление неактивированными («дремлющими») договорами.

13.4.7. Разработка планов и процедур восстановления

Планы должны быть разработаны в деталях, и стать официальными документами, т. к. Планы восстановления требуют поддержки, и все изменения в них должны согласовываться заинтересованными сторонами. Эта информация также должна доводиться до сведения всех участников. Основные проблемы связаны с изменениями в инфраструктуре и Изменениями Уровней Сервиса. Например, переход на новую платформу среднего класса² может привести к тому, что не будет эквивалентного оборудования в резервном центре «теплого», внешнего старта. По этой причине Процесс Управления Конфигурациями играет важную роль в мониторинге базисных конфигураций с учетом Плана восстановления. В плане также должны быть определены процедуры, необходимые для его выполнения.

План восстановления

План восстановления должен включать все виды деятельности по восстановлению бизнес-активности и ИТ-услуг:

- **Введение** — описание структуры плана и предполагаемых средств восстановления.
- **Обновление** — описание процедур и соглашений по поддержке актуальности плана и отслеживанию изменений в инфраструктуре.
- **Маршрутный лист** — план делится на разделы, каждый из которых определяет действия, выполняемые конкретной группой специалистов. Маршрутный лист показывает, какие разделы плана должны быть направлены в каждую группу.
- **Начало восстановления** — описание времени и условий начала действия плана.
- **Классификация чрезвычайных обстоятельств** — если в плане дается описание процедур на случай различных чрезвычайных обстоятельств, то они должны быть описаны с точки зрения их серьезности (незначительные, среднего уровня серьезности, серьезные), длительности (день, неделя, месяцы) и уровня повреждений (незначительные, ограниченные, серьезные).

¹ Fault-tolerant systems.

² Midrange platform.

▪ **Разделы для участвующих групп специалистов** — план должен быть разделен на шесть разделов — по количеству областей действия и закрепленных на за ними групп специалистов:

- *Администрация* — как и когда вводить план в действие, какие руководители и специалисты участвуют в нем, где находится центр управления?

- *ИТ-инфраструктура* — аппаратное и программное обеспечение, телекоммуникационные средства, включенные в систему восстановления и соответствующие процедуры, а также неактивированные («дремлющие») договоры на закупку новых ИТ-компонентов.

- *Персонал* — персонал, необходимый для работы в резервном центре, возможно, средства транспортировки и размещение персонала, если резервный центр расположен удалено от основного месторасположения.

- *Безопасность* — инструкции по защите от краж, пожаров и взрывов, как в основном здании, так и на удаленной площадке, а также информация о внешних хранилищах, таких как склады и подвалы.

- *Площадки восстановления* — информация о договорах, персонале с указанием конкретных функций, системе безопасности и транспорте.

- *Возврат к нормальным условиям* — процедуры восстановления нормальной инфраструктуры (например, здания), условия, при которых начинают действовать эти процедуры и соответствующие неактивированные («дремлющие») контракты.

Процедуры

Процедуры разрабатываются на основе Плана восстановления. Они должны быть эффективными¹, так, чтобы каждый мог выполнять работы по восстановлению, следуя этим процедурам. Процедуры должны включать:

- установку и тестирование технических средств и сетевых компонентов;
- восстановление приложений, баз данных и других данных.

Эти и другие необходимые процедуры должны прилагаться к Плану восстановления.

13.4.8. Начальное тестирование

Начальное тестирование — критически важный аспект процесса ITSCM. Тесты следует проводить в начале работы, потом после проведения значительных изменений и затем, как минимум, один раз год. ИТ-подразделения отвечают за тестирование эффективности планов и процедур в отношении ИТ-элементов. Тесты могут проводиться с предварительным объявлением или без него.

13.4.9. Обучение и осведомление

Обучение персонала ИТ-подразделения и других отделов компании и осведомленность всего персонала организации являются важными условиями успешной реализации Процесса Управления Непрерывностью ИТ-сервисов.

Персонал ИТ-подразделения должен проводить обучение других членов команды восстановления бизнеса, незнакомых с вопросами информационных технологий, чтобы они могли оказать необходимую поддержку при проведении восстановительных работ. Обучение и тестирование должно охватывать как центральные, так и удаленные средства, предусмотренные на случай чрезвычайных обстоятельств.

13.4.10. Анализ и аудит

Следует регулярно проводить аудит и проверять актуальность всех планов. Такая проверка затрагивает все аспекты Процесса Управления Непрерывностью ИТ-сервисов. В области ИТ

¹ Effective.

такой аудит должен проводиться при каждом значительном изменении ИТ-инфраструктуры, например, при вводе в операционную среду новых систем и сетей и появлении новых поставщиков. Аудит также должен проводиться при любом изменении стратегии ИТ-подразделения или бизнеса. Организации, где происходят быстрые и частые изменения, могут внедрить регулярную программу по проверке концепции процесса ITSCM. Любые изменения в планах и стратегии, появившиеся в результате проведения таких проверок, должны быть реализованы под руководством Процесса Управления Изменениями.

13.4.11. Тестирование

Необходимо проводить регулярное тестирование Плана восстановления, подобно объявлению учебных тревог на борту корабля. Если в компании изучение плана начинается после того, как произошла чрезвычайная ситуация, то, вероятнее всего, у такой организации будет немало проблем с восстановлением. Тестирование позволяет выявить слабые места плана и изменения, которые не были учтены. В некоторых случаях можно проводить тестирование изменений на средствах восстановления прежде, чем вводить их в действующую ИТ-инфраструктуру.

13.4.12. Управление Изменениями

Процесс Управления Изменениями играет важную роль в поддержании актуальности Планов восстановления. Необходимо проводить анализ воздействия любого изменения на План восстановления.

13.4.13. Обеспечение гарантий¹

Обеспечение гарантий работоспособности процесса означает проверку соответствия качества процесса (процедур и документации) бизнес-потребностям компании.

13.5. Управление Процессом

Эффективное Управление Процессом базируется на отчетах для руководства, критических факторах успеха и ключевых показателях качества.

13.5.1. Отчеты для руководства

В случае возникновения чрезвычайной ситуации предоставляются отчеты о причинах и последствиях чрезвычайной ситуации и действиях по ее разрешению. Любое выявленное при этом слабое место будет учтено в Планах по улучшению сервисов.

В отчеты для руководства по данному процессу также должны быть включены отчеты о тестировании Плана восстановления. Должны также составляться отчеты о произведенных изменениях в плане по восстановлению как результатах изменения каких-либо частей ИТ-инфраструктуры.

13.5.2. Критические факторы успеха и ключевые показатели качества

Успех Процесса Управления Непрерывностью ИТ-сервисов зависит от следующих факторов:

- наличия эффективного Процесса Управления Конфигурациями;
- поддержки процесса всеми в компании;
- наличия современных эффективных инструментальных средств;
- проведения специального обучения для всех участников данного процесса;
- регулярного тестирования плана восстановления без предварительного уведомления.

¹ Assurance.

Ключевыми показателями качества являются:

- количество выявленных ошибок в планах восстановления;
- потеря дохода компании в результате чрезвычайной ситуации;
- стоимость процесса.

13.5.3. функции и роли

Задачи Руководителя Процесса Управления Непрерывностью ИТ-сервисов состоят во внедрении и обеспечении поддержки процесса ITSCM для постоянного выполнения всех требований по Управлению Непрерывностью Бизнеса (BCM) и представлении функций ИТ-сервисов в рамках процесса BCM.

В данном процессе можно определить несколько ролей и видов ответственности, а также установить различие между ответственностью в обычных условиях и ответственностью в кризисных ситуациях.

Роль	Ответственность в обычных условиях	Ответственность в кризисных ситуациях
Совет директоров	Инициация процесса BCM Выделение персонала и ресурсов Выработка политики Определение полномочий в рамках процесса	Руководство действиями в кризисной ситуации Принятие корпоративных/бизнес решений
Высшее руководство	Управление процессом ITSCM Утверждение планов, отчетов о тестировании и т.д. Коммуникации в компании и создание осведомленности в компании Интеграция процесса ITSCM в процессе BCM	Координация и арбитраж (принятие окончательных решений) Предоставление персонала, ресурсов и финансовых средств.
Руководство	Проведение анализа рисков Определение, какие должны быть результаты работы Составление проектов договоров Руководство тестированием, оценкой и составлением отчетов	Приведение в действие механизмов восстановления и обеспечения Руководство командами непрерывности Составление отчетов
Руководители команд и члены команд	Проработка способов достижения результатов работы Ведение переговоров по предоставляемым услугам Проведение тестов, оценок и составление отчетов	Разработка и внедрение процедур Реализация плана восстановления

Таблица 13.1. Примеры видов ответственности в рамках Процесса Управления Непрерывностью ИТ-сервисов

13.6. Проблемы и затраты

13.6.1. Затраты

Основные затраты, связанные с реализацией Процесса Управления Непрерывностью следующие:

- затраты времени и средств на инициацию, разработку и внедрение процесса ITSCM.
- затраты на организацию Управления Рисками и связанное с этим дополнительное аппаратное обеспечение. Эти расходы можно сократить, если включить эти действия в сферу деятельности Процесса Управления Доступностью на этапе разработки новых конфигураций.
- переходящие затраты на поддержку выбранных способов восстановления, такие как плата по Внешним Договорам по «горячему» старту, затраты на организацию тестирования и плата за период поддержания в готовности средств восстановления.
- повторяющиеся операционные расходы на тестирование, аудит и корректировку планов.

Эти расходы возникают только после того, как сделан обоснованный выбор и проведено сравнение с возможными расходами в случае отказа от создания Плана восстановления. Хотя затраты на поддержку такого плана могут показаться высокими, часто они оказываются вполне сопоставимыми с общими расходами на страхование от пожаров и воровства. Более того, эффективный процесс ITSCM может помочь уменьшить расходы на страхование.

13.6.2. Проблемы

При внедрении данного процесса могут возникнуть следующие проблемы:

- **Ресурсы** — организация должна предоставить дополнительные мощности проектной команде для разработки и тестирования плана.
- **Серьезность намерений (обязательства)** — ежегодные расходы на процесс должны быть включены в бюджеты организации, для чего требуется твердое намерение руководства поддерживать Процесс Управления Непрерывностью ИТ-сервисов.
- **Доступ к средствам восстановления** — для всех обсужденных выше способов восстановления требуется проведение регулярного тестирования соответствующих средств. Поэтому заключаемые договоры должны обеспечивать регулярный доступ ИТ-организации к средствам восстановления.
- **Оценка потерь** — некоторые потери, такие как потеря репутации, нельзя измерить в денежном выражении.
- **Составление бюджета** — не всегда удастся добиться понимания необходимости в дорогих средствах восстановления функциональности, иногда происходит сокращение Планов восстановления.
- **Отсутствие обязательств со стороны бизнес-руководителя** — это ведет к неудаче в разработке процесса ITSCM, хотя заказчик может полагать, что все необходимое сделано.
- **Постоянное откладывание** — это бывает в тех случаях, когда отсутствует большинство составляющих процесса и, как следствие этого, реализация процесса постоянно откладывается. В таких случаях на вопрос о Процессе Управления Непрерывностью ИТ-сервисов даются ответы: «Да. Мы встречаемся по этому вопросу на следующей неделе», «Мы собирается создать комиссию специально по данному вопросу» и тому подобное.
- **Черный ящик** — это бывает в тех случаях, когда поставщик ИТ-услуг отказывается от ответственности, а также прекращает управлять готовностью процесса: «Кто-то еще этим занимается». Поскольку организация затратила много средств или передала часть своих операций поставщику, руководство надеется, что затраченные деньги обеспечат возможность восстановления или же что у поставщика есть планы, которые помогут восстановить бизнес после чрезвычайной ситуации.
- **ИТ-подразделение** — в своей работе должно руководствоваться действительными пожеланиями и требованиями бизнеса, а не своими предположениями.
- **Знание бизнеса** — важно, чтобы бизнес поддерживал разработку процесса ITSCM путем определения основных направлений работы.
- **Отсутствие осведомленности в компании** — необходимо, чтобы вся организация знала о значимости процесса ITSCM. Без информирования персонала и его поддержки процесс обречен на неудачу.

Глава 14

Управление Доступностью

14.1. Введение

В настоящее время развитие технологии идет нарастающими темпами. По этой причине во многих организациях необходимое для работы аппаратное и программное обеспечение становится более многочисленным и разнообразным, несмотря на все попытки его стандартизации. Старые и новые технологии вынуждены существовать вместе. Такое сосуществование приводит к появлению дополнительных сетевых средств, интерфейсов и средств коммуникации. Происходит усиление зависимости бизнеса от технологий.

Несколько часов простоя компьютера могут иметь серьезные последствия для бизнеса и репутации компании на рынке, особенно сейчас, когда Интернет превращается в электронный вариант рынка. В этом электронном мире конкурентов друг от друга отделяет простое нажатие на клавишу «мыши». В этой связи особенно важным фактором становится степень удовлетворенности заказчиков. Эта одна из причин, почему в настоящее время вычислительные системы должны быть доступны 24 часа в сутки семь дней в неделю.

14.1.2. Основные понятия

На рис. 14.1 схематично представлены базовые понятия процесса Управления Доступностью.

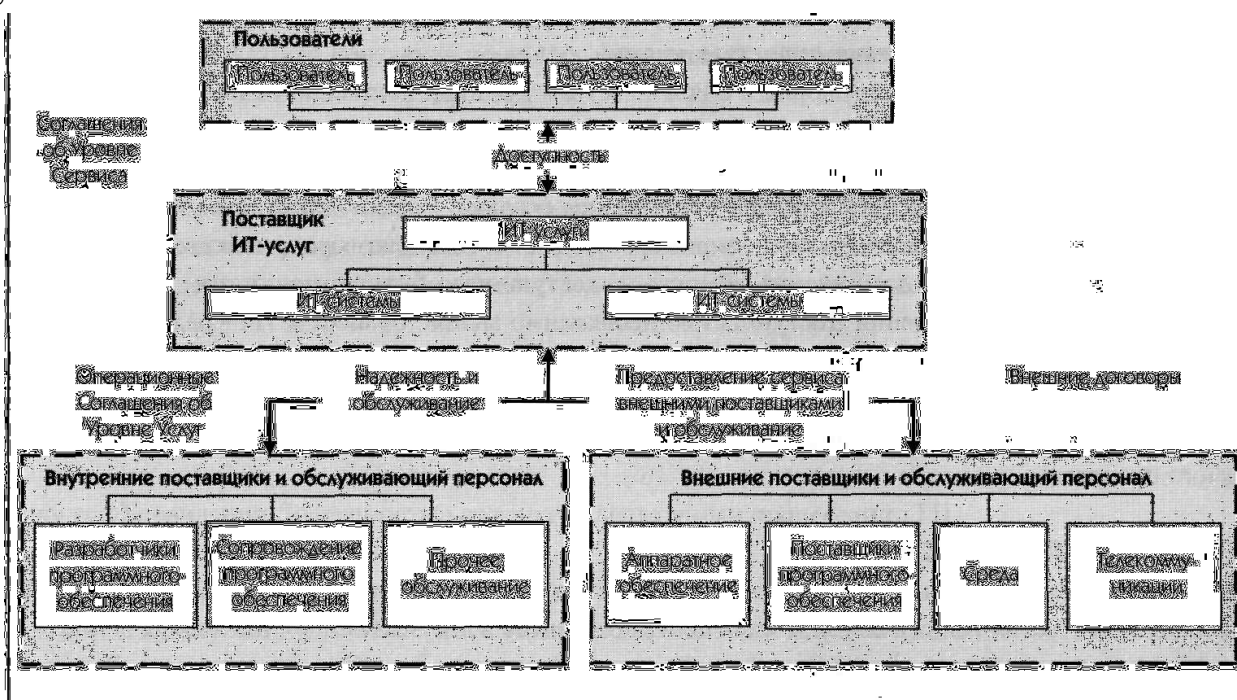


Рис. 14.1. Концептуальные понятия процесса Управления Доступностью (источник: OGC)

Доступность

Высокий Уровень Доступности означает, что заказчик имеет практически постоянный доступ к ИТ-сервису благодаря сокращению времени простоя и быстрому восстановлению предоставления услуг. Уровень Доступности определяется с помощью метрик. Доступность сервиса зависит от:

- сложности ИТ-инфраструктуры;
- надежности компонентов;
- способности быстро и эффективно реагировать на сбои;
- качества обслуживания и качества работы поддерживающих организаций и поставщиков;

- качества и границ компетенции процессов операционного управления.

Надежность¹

Надежность, в контексте данного процесса, означает доступность сервиса в течение согласованного периода времени без каких-либо сбоев. Эта концепция включает в себя понятие устойчивости². Надежность сервиса будет возрастать, если предпринимать превентивные меры против возникновения простоев. Надежность сервиса является статистическим показателем и определяется сочетанием следующих факторов:

- надежность компонентов, используемых для предоставления сервиса;
- способность сервиса или его компонентов эффективно функционировать, несмотря на сбой одной или нескольких подсистем (устойчивость);
- профилактическое обслуживание для предотвращения простоев.

Обслуживание³

Понятия «обслуживание» и «способность к восстановлению»⁴ предполагают выполнение работ по обеспечению функционирования сервиса и его восстановлению после сбоев, а также проведение профилактического обслуживания и регламентных (плановых) проверок, а именно;

- принятие мер по предотвращению сбоев;
- своевременное обнаружение сбоев;
- проведение диагностики, включая автоматическую самодиагностику компонентов;
- ликвидация сбоев;
- восстановление функционирования после сбоя;
- восстановление сервиса.

Предоставление сервиса внешними поставщиками⁵

Данное понятие относится к договорным обязательствам внешних поставщиков сервиса (подрядчики, сторонние организации). Договорами определяется поддержка, которая будет обеспечена сервисам, поставляемым внешними организациями (аутсорсинг). Поскольку это только часть ИТ-сервиса, данный термин не относится к общей доступности сервиса. Если подрядчик несет ответственность за сервис в целом, как это бывает, например, при заключении договора хозяйственного обеспечения, тогда термины «Предоставление сервиса» и «доступность» будут синонимами. Для эффективного Управления Доступностью необходимо знание бизнеса и ИТ-среды. Важно понять, что доступность нельзя просто «купить»: доступность должна закладываться на самых ранних этапах разработки и внедрения. В конечном счете доступность зависит от сложности инфраструктуры, надежности компонентов, профессионализма ИТ-организации и ее подрядчиков и от качества самого процесса.

14.2. Цели процесса

Целью Процесса Управления Доступностью является обеспечение рентабельного и согласованного Уровня Доступности ИТ-сервиса, который поможет бизнесу в достижении поставленных целей. Такое определение цели процесса означает, что потребности заказчика (бизнеса) должны соответствовать тому, что могут предложить ИТ-инфраструктура и организация. Если имеется расхождение между спросом и предложением, тогда Процесс Управления Доступностью должен предложить выход из такой ситуации. Более того, данный

¹ Reliability.

² Resilience - устойчивость: способность сервиса сохранять доступность при сбое одного или нескольких ИТ-компонент. - Прим. ред.

³ Maintainability.

⁴ Recoverability.

⁵ Serviceability.

процесс гарантирует оценку достигнутых Уровней Доступности и их дальнейшее совершенствование в случае необходимости. Это означает, что в рамках процесса выполняются как проактивные, так и реактивные виды деятельности. При разработке процесса следует исходить из следующих предпосылок:

- Использование Процесса Управления Доступностью необходимо для достижения наибольшей удовлетворенности заказчика. Доступность и надежность — два показателя, во многом определяющие восприятие предоставляемых услуг заказчиком.
- Высокая степень доступности не означает отсутствие сбоев. Управление Доступностью в основном отвечает за профессиональное реагирование на такие нежелательные ситуации.
- Проектирование процесса требует не только полного понимания информационных технологий, но понимания процессов и услуг заказчика. Достижение целей возможно только путем сочетания этих двух аспектов.

У Процесса Управления Доступностью широкая сфера действия, охватывающая новые и уже существующие услуги, отношения с внешними и внутренними поставщиками, все компоненты инфраструктуры (аппаратное и программное обеспечение, сети и т. д.) и влияющие на доступность организационные аспекты, такие как Уровень Знаний Персонала, управленческие процессы, процедуры и инструментальные средства.

14.2.1. Преимущества использования процесса

Основное преимущество, которое дает Процесс Управления Доступностью, состоит в том, что услуги, разработанные, внедренные и находящиеся под Управлением ИТ-организации, отвечают требованиям, предъявляемым к доступности сервиса. Полное понимание бизнес-процессов заказчика и информационных технологий в сочетании с постоянным стремлением максимально расширить доступность сервиса в разумных пределах могут во многом содействовать формированию реальной культуры сервиса. Другие преимущества данного процесса состоят в следующем:

- создание единой точки контактов по вопросам доступности продуктов и услуг и наличие одного человека, отвечающего за эти вопросы;
- гарантируется соответствие новых продуктов и услуг предъявляемым к ним требованиям и согласованному с заказчиком стандарту доступности;
- Уровень Затрат поддерживается на приемлемом уровне;
- постоянный мониторинг стандартов доступности и их совершенствование по мере необходимости;
- в случае недоступности сервиса выполнение восстановительных мероприятий, соответствующих ситуации;
- уменьшение количества отказов в доступе к системам и сокращение периода недоступности сервиса;
- смещение акцентов с исправления дефектов на улучшение сервиса;
- простота обоснования добавочной стоимости для ИТ-организации.

Процесс Управления Доступностью связан со следующими процессами ИТIL.

Управление Уровнем Сервиса

Процесс Управления Уровнем Сервиса осуществляет согласование и Управление Соглашениями об Уровне Сервиса, в которых Доступность является одним из важнейших параметров.

Управление Конфигурациями

Процесс Управления Конфигурациями располагает информацией об инфраструктуре и может предоставлять ценную информацию Процессу Управления Доступностью.

Управление Мощностями

Изменение Мощностей часто влияет на доступность сервиса, а изменения параметров доступности затрагивают параметры мощности сервиса. Процесс Управления Мощностями располагает обширной информацией, включая информацию об инфраструктуре. Поэтому эти процессы часто обмениваются информацией о сценариях модернизации ИТ-компонентов или их вывода из операционной среды, а также о тенденциях в сфере доступности, которые могут вызвать изменения в требованиях к мощностям сервиса.

Управление Непрерывностью Сервиса

Процесс Управления Доступностью не несет ответственности за восстановление бизнес-процессов после катастрофы. Это обязанность Процесса Управления Непрерывностью ИТ-сервиса, который предоставляет Процессу Управления Доступностью информацию о наиболее важных бизнес-процессах. На практике бывает так, что многие меры по улучшению доступности сервиса приводят к улучшению непрерывности ИТ-сервиса и наоборот.

Управление Проблемами

Процесс Управления Проблемами непосредственно участвует в обнаружении причин существующих и потенциальных проблем в сфере доступности сервиса и в их устранении.

Управление Инцидентами

Процесс Управления Инцидентами определяет способ разрешения инцидентов. Этот процесс предоставляет отчеты, содержащие информацию о затратах времени на разрешение инцидентов, ремонт и т. д. Соответствующая информация используется для определения достигнутого Уровня Доступности.

Управление Безопасностью

Процесс Управления Доступностью тесно связан с Процессом Управления Безопасностью, в котором основными вопросами являются:

- Конфиденциальность;
- Целостность;
- Доступность.

Критерии безопасности следует учитывать при определении требований к доступности. Процесс Управления Доступностью может дать ценную информацию Процессу Управления Безопасностью, особенно о новых услугах.

Управление Изменениями

Процесс Управления Доступностью информирует Процесс Управления Изменениями о вопросах обслуживания новых услуг и их элементов и инициирует проведение изменений, обусловленных вопросами доступности. Процесс Управления Изменениями информирует Процесс Управления Доступностью о содержании Перспективного Плана Изменений (FSC).

14.3. Процесс

Для соответствия стандартам высокой доступности сервиса производится дублирование важных компонентов там, где это возможно, и используются системы обнаружения и устранения сбоев. Часто в случае обнаружения дефекта начинают автоматически действовать резервные системы. Тем не менее в таких ситуациях также необходимо принимать организационные меры, и их может обеспечить Процесс Управления Доступностью.

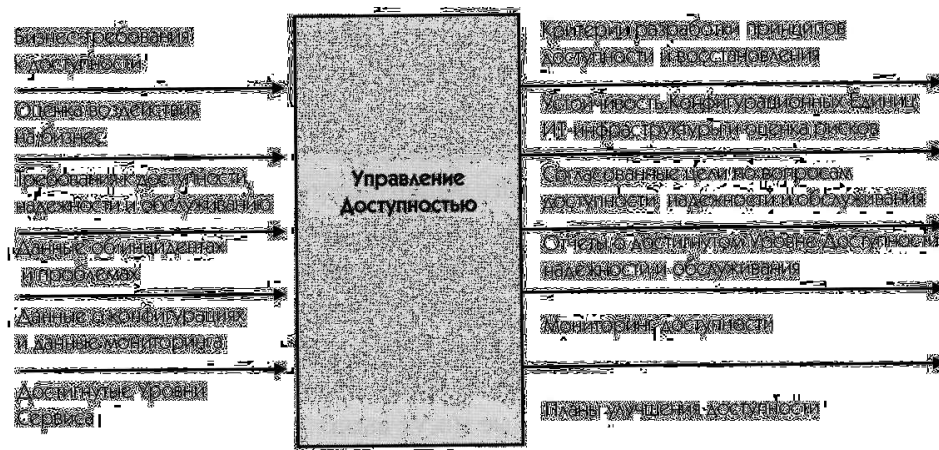


Рис. 14.2. Входы и выходы Процесса Управления Доступностью (источник: OGC)

Процесс Управления Доступностью начинает действовать после того, как бизнес четко определил свои требования к доступности сервиса. Это непрерывный процесс, который заканчивается только тогда, когда прекращается предоставление сервиса.

Входами для Процесса Управления Доступностью являются (рис. 14.2):

- требования бизнеса к доступности;
- оценка влияния на все бизнес-процессы, поддерживаемые ИТ;
- требования к доступности, надежности и обслуживанию ИТ-компонентов инфраструктуры;
 - данные о неисправностях, затрагивающих услуги или их компоненты, обычно в форме записей и отчетов об инцидентах и проблемах;
 - данные о конфигурациях услуг и их компонентах и данные мониторинга;
 - достигнутые Уровни Сервиса в сравнении с согласованными уровнями для всех услуг, оговоренных в соглашении о предоставлении сервиса.

Выходы:

- критерии разработки архитектуры для обеспечения доступности и восстановления новых и улучшаемых ИТ-услуг;
- технология, обеспечивающая устойчивость инфраструктуры и позволяющая уменьшить или устранить воздействие дефектных компонентов;
- гарантии доступности, надежности и обслуживания компонентов инфраструктуры, необходимые для предоставления ИТ-сервиса;
- отчеты о достигнутых Уровнях Доступности, надежности и обслуживания;
- требования к мониторингу доступности, надежности и обслуживания;
- план обеспечения доступности¹ для проведения проактивного улучшения ИТ-инфраструктуры.

14.4. Виды деятельности

В рамках Процесса Управления Доступностью выполняется ряд ключевых видов деятельности, связанных с планированием и мониторингом, а именно:

- Планирование
 - определение требований к доступности сервиса;
 - проектирование систем для достижения требуемого Уровня Доступности;

¹ Availability Plan.

- проектирование систем для достижения требуемой способности восстановления¹;
- вопросы безопасности;
- управление обслуживанием;
- разработка Плана Доступности.
- Мониторинг
- проведение измерений и составление отчетов. Ниже дается описание основных видов деятельности.

14.4.1. Определение требований к доступности сервиса

Данный вид работ должен выполняться до заключения соглашения об Уровне Сервиса, и он затрагивает новые ИТ-услуги и изменения в уже существующих услугах. ИТ-организация должна определить как можно быстрее, будет ли она выполнять эти требования и если да, то как. Во время выполнения этого вида деятельности определяются:

- ключевые бизнес-функции;
- согласованный период простоя ИТ-сервиса;
- количественная оценка требований к доступности сервиса;
- количественная оценка воздействия незапланированного простоя на бизнес-функции;
- рабочие часы заказчика;
- соглашения об «окнах» для планового обслуживания.

Четкое определение требований к доступности сервиса на ранних этапах позволяет избежать недоразумений и неправильного толкования договоренностей на более поздних этапах. Требования заказчика необходимо сопоставлять с теми, которые организация может предоставить. Если выявляется несоответствие, то следует определить влияние такого несоответствия на стоимость услуг.

14.4.2. Проектирование систем для достижения требуемого Уровня Доступности

Следует как можно раньше выявить различные виды уязвимости, влияющие на доступность. Это позволит избежать неоправданно высокой стоимости разработки, незапланированных расходов на более поздних этапах, наличия Единой точки сбоя² (SPOF), дополнительных затрат по счетам поставщиков и задержек с выпуском релизов.

Хорошее проектирование, выполненное с учетом стандартов доступности, позволит заключить с поставщиками эффективные договоры на обслуживание. При проектировании используется ряд методов, таких как Анализ степени влияния сбоя компонента³ (CFIA — см. раздел 14.4.9) для выявления отказов, вызванных наличием SPOF, методика ССТА по анализу и Управлению Рисками⁴ (CRAMM — см. главу «Управление Непрерывностью ИТ-сервиса») и методы моделирования. Если требования стандартов доступности не могут быть удовлетворены, лучший путь — попытаться внести соответствующие усовершенствования в проект. В обеспечении соответствия стандартам может помочь использование дополнительных технологий, других методов, инструментальных средств разработки, другой стратегии Управления Релизами, улучшение или изменение процесса проектирования.

Если требования особенно высоки, то можно попытаться использовать другую отказоустойчивую технологию, другие Процессы Управления Услугами (Управление Инцидентами, Проблемами и Изменениями) или дополнительные ресурсы Сервис-менеджмента. Выбор варианта во многом зависит от имеющихся финансовых средств.

¹ Recoverability.

² Single points of failures - SPOF.

³ Component Failure Impact Analysis — CFIA.

⁴ CSTA Risk Analysis and Management - CRAMM

14.4.3. Проектирование систем для достижения требуемого Уровня Обслуживания

Поскольку постоянная доступность бывает редко достижима, следует учитывать периоды возможной недоступности сервиса. При прерывании сервиса важно быстро и правильно устранить сбой и попытаться достигнуть согласованных стандартов доступности. Проектирование процедур восстановления включает в себя такие аспекты, как использование эффективного Процесса Управления Инцидентами и соответствующие процедуры эскалации, оповещения, резервного копирования и восстановления.

Задачи, ответственность и полномочия должны быть четко определены.

14.4.4. Ключевые вопросы безопасности

Безопасность и надежность тесно взаимосвязаны. Недостаточная проработка вопросов информационной безопасности может повлиять на доступность сервиса. Высокий Уровень Доступности должен поддерживаться эффективно действующей системой информационной безопасности. На этапе планирования следует учитывать вопросы безопасности и анализировать их воздействие на предоставление услуг.

Среди вопросов могут быть следующие:

- определение лиц, имеющих право доступа в защищенные области;
- определение видов авторизации.

14.4.5. Управление Обслуживанием

В обычной практике всегда бывают запланированные периоды недоступности сервиса. Эти периоды можно использовать для проведения превентивных действий, таких как обновление программного и аппаратного обеспечения, а также выполнения изменений. Однако в условиях непрерывного бизнеса становится все труднее определить периоды, выделяемые для обслуживания. Проектирование, реализация и контроль деятельности по обслуживанию систем стали одним из важных направлений работы Процесса Управления Доступностью.

Обслуживание следует проводить в такие периоды, когда степень его воздействия на предоставление услуг является минимальной. Это значит, что необходимо заранее определить цели обслуживания, период его проведения, и какие работы при этом будут выполняться (для этого можно использовать метод Анализа влияния отказа компонентов — CFIA¹). Такая информация об обслуживании очень важна для Процесса Управления Изменениями и для других процессов.

14.4.6. Проведение измерений и составление отчетов

Проведение измерений и составление отчетов являются важными видами деятельности в Процессе Управления Доступностью, т. к. они создают основу для верификации соглашений о предоставлении сервиса, для разрешения проблем и выработки предложений по улучшению сервиса.

*Если Вы не измеряете, Вы не можете управлять.
Если Вы не измеряете, Вы не можете улучшить.
Если Вы не измеряете, Вам, вероятно, все равно.
Если Вы не можете влиять, то не стоит и измерять.*

Цикл жизни инцидента включает в себя следующие этапы:

- **Возникновение инцидента:** время, когда пользователь узнал о сбое или когда сбой был обнаружен (автоматически или вручную).

¹ Component Failure Impact Analysis — CFIA.

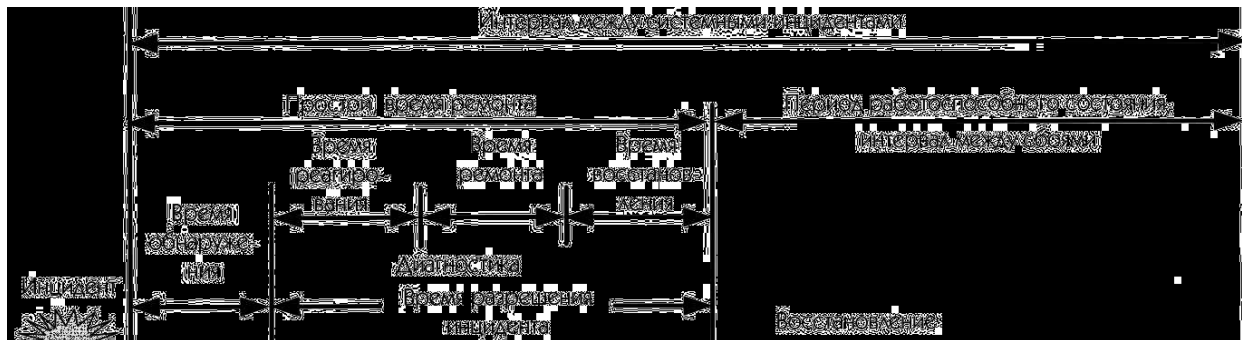
- **Обнаружение:** поставщик сервиса проинформирован о сбое. Инцидент получает статус «Сообщено». Затраченное на это время известно как время обнаружения.

- **Реагирование:** поставщику сервиса необходимо время, чтобы прореагировать на инцидент. Это время реагирования, оно используется для проведения диагностики, за которой следует выполнение ремонтных работ. В Процесс Управления Инцидентами входят такие виды работ, как Прием и Регистрация инцидентов, Классификация, Сопоставление, Анализ и Диагностика.

- **Ремонт:** поставщик сервиса восстанавливает компоненты, которые вызвали сбой.

- **Восстановление сервиса:** сервис восстановлен. При этом выполняются такие работы, как конфигурирование и инициализация, и затем производится восстановление предоставления сервиса пользователям.

На рис. 14.3 показаны периоды времени, которые поддаются измерению.



Время/жизненный цикл

Рис. 14.3. Измерение доступности (источник: OGC)

Как видно из рисунка, время реагирования ИТ-организации и внешних подрядчиков является одним из факторов, определяющих время простоя. Поскольку этот фактор непосредственно влияет на качество сервиса и ИТ-организация может его контролировать, то в соглашения об Уровне Сервиса можно включать договоренности относительно времени реагирования. При измерениях можно брать средние значения для получения правильного представления о соответствующих параметрах. Средние значения можно использовать для определения достигнутого Уровня Сервиса и для оценки ожидаемой в будущем доступности. Эту информацию можно использовать при разработке Планов Улучшения Сервиса.

В Процессе Управления Доступностью, как правило, используются следующие метрики:

- **Среднее время ремонта (Mean Time to Repair — MTTR):** среднее время между возникновением сбоя и восстановлением сервиса, также известное как «простой». Оно складывается из времени обнаружения сбоя и времени разрешения сбоя. Данная метрика относится к таким аспектам сервиса, как способность восстановления¹ и обслуживаемость².

- **Среднее время между сбоями (Mean Time Between Failures — MTBF):** среднее время между восстановлением после одного сбоя и возникновением другого, также известное как «период работоспособного состояния» (uptime). Данная метрика относится к надежности сервиса.

- **Среднее время между системными инцидентами (Mean Time Between System Incidents — MTBSI):** среднее время между двумя последовательными инцидентами. Данная метрика представляет собой сумму двух метрик MTTR и MTBF.

Соотношение метрик MTBF и MTBSI помогает понять, имело ли место много незначительных сбоев или было несколько серьезных нарушений в работе.

¹ Recoverability

² Serviceability.

В отчеты о доступности сервиса могут быть включены следующие метрики:

- Коэффициент доступности (или недоступности) сервиса, выраженный в метриках MTTR, MTBSI и MTBF;
- общее время работоспособного состояния и время простоя;
- количество сбоев;
- дополнительная информация о сбоях, которые могут привести в настоящее время или в будущем к более высокому Уровню Недоступности Систем, чем было заранее согласовано.

Проблема составления отчетов состоит в том, что представленные выше метрики могут не восприниматься заказчиком. Поэтому отчеты о доступности сервиса должны составляться с точки зрения заказчика. Отчет в первую очередь должен давать информацию о доступности сервиса для наиболее важных бизнес-функций и о доступности данных (т. е. давать бизнес-представления), а не о доступности технических ИТ-компонентов. Отчеты должны быть написаны на понятном заказчику языке.

14.4.7. Разработка Плана Обеспечения Доступности

Одним из основных результатов процесса является План Доступности¹. Это долгосрочный План Обеспечения Доступности Сервиса на несколько последующих лет, он не является Планом Внедрения Процесса Управления Доступностью.

План — это живой документ. В начале он должен дать описание текущей ситуации, а затем в него можно включать рекомендации и конкретные виды работ по улучшению существующих услуг, а также предложения по вводу новых услуг и их обслуживанию. Для составления полного и точного плана необходимо взаимодействие с такими Процессами, как Управление Уровнем Сервиса, Управление Непрерывностью ИТ-сервиса, Управление Финансами ИТ-сервиса, а также с Управлением Разработкой Приложений (напрямую или через Процесс Управления Изменениями).

14.4.8. Инструментальные средства

Для достижения эффективности Процесс Управления Доступностью должен использовать ряд инструментальных средств следующего назначения:

- определение времени простоя;
- фиксация исторической информации;
- создание отчетов;
- статистический анализ;
- анализ воздействия.

Процесс Управления Доступностью берет информацию из записей Процесса Управления инцидентами, Базы Данных CMDB и из Базы Данных Процесса Управления Мощностями (CL)², Эта информация может храниться в специальной Базе Данных Процесса Управления Доступностью.

14.4.9. Методы и методики

В настоящее время существует широкий спектр методов и методик Управления Доступностью, которые помогают в проведении планирования, улучшения доступности и в составлении отчетов. Наиболее важные из них приведены ниже.

¹ Availability plan.

² Availability Management Database — AMDB

Анализ влияния отказа компонентов (CFIA)¹

Данный метод предполагает использование матрицы доступности стратегических компонентов и их ролей в каждой услуге. При разработке такой матрицы очень полезной может оказаться база данных CMDB.

Пример матрицы CFIA на рис. 14.4 показывает, что Конфигурационные Единицы, которые для многих услуг помечены символом «X», являются важными элементами ИТ-инфраструктуры (анализ по горизонтали) и что услуги, часто отмечаемые символом «X», являются комплексными и подвержены сбоям (анализ по вертикали). Этот метод также можно применять для изучения степени зависимости от сторонних организаций (усовершенствованный метод CFIA).

Конфигурационная единица	Услуга А	Услуга Б
PC № 1		
PC № 2		
Кабель № 1		
Кабель № 2		
Разъем № 1		
Разъем № 2		
Сегмент сети Ethernet		
Маршрутизатор		
Канал глобальной сети (WAN)		
Маршрутизатор		
Сегмент		
Сетевой информационный центр		
Сервер		
Системное программное обеспечение		
Приложения		
База данных		

X - сбой/дефект означает, что услуга недоступна

A - безотказная конфигурация

B — безотказная конфигурация, с переключением

« » — нет воздействия

Рис. 14.4. Матрица CFIA (источник: OGC)

Анализ дерева неисправностей² (FTA)

Анализ дерева неисправностей используется для определения цепочки событий, приводящих к сбою ИТ-сервиса. Для каждой услуги изображается отдельное дерево с использованием символов Буля. Дерево анализируется снизу вверх. Метод FTA выделяет следующие события:

- **Основные события:** входы на схеме (обозначены кружочками), такие как отключение электропитания и ошибки операторов. Эти события не исследуются.
- **Результирующие события:** узловая точка на схеме, появившаяся в результате объединения двух более ранних событий.
- **Условные события:** события, которые происходят только при определенных условиях, таких как отказ кондиционера.
- **Запускающее событие:** события, которые приводят к возникновению других событий, такие как автоматическое отключение, вызванное сигналом источника бесперебойного питания.

События можно объединять с логическими операциями, такими как:

- операция AND (И): результирующее событие произойдет, если будут присутствовать все входы одновременно;
- операция OR (ИЛИ): результирующее событие произойдет, если будет иметь место один или несколько входов;

¹ Component Failure Impact Analysis — CFIA.

² Fault Tree Analysis- FTA.

- операция XOR (Исключающее ИЛИ): результирующее событие произойдет, если будет иметь место только один вход/причина;
- операция Inhibit (Запрет): результирующее событие произойдет, если не будут выполнены входные условия.

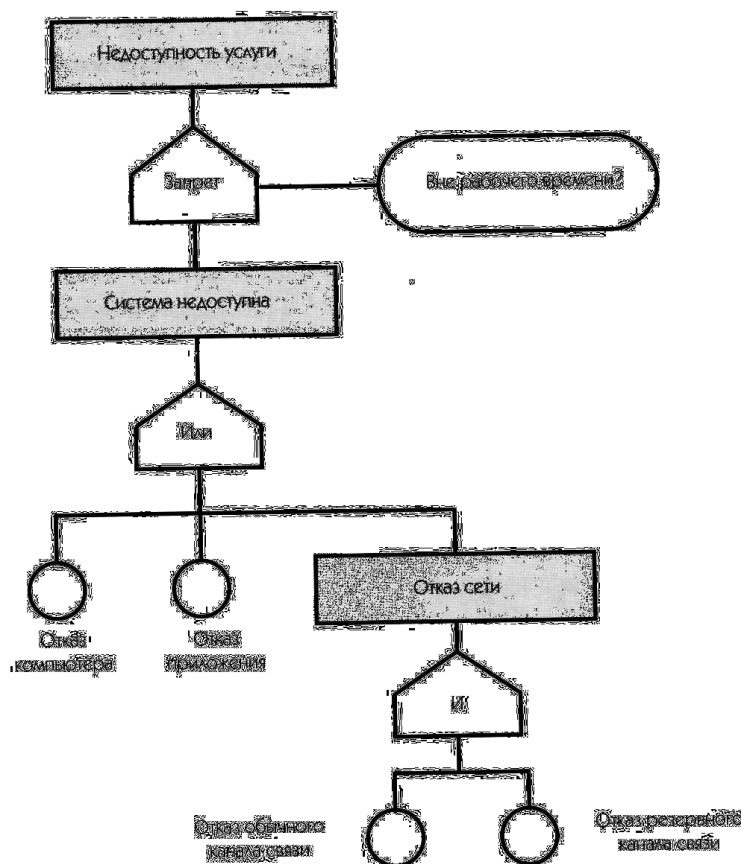


Рис. 14.5. Анализ дерева дефектов/сбоев (источник: OGC)

Метод Анализа и Управления Рисками¹ (CRAMM)

Данный метод рассматривался в главе, посвященной Управлению Непрерывностью ИТ-сервиса.

Расчеты доступности сервиса

Описанные выше метрики можно использовать при заключении соглашений о доступности сервиса с заказчиками. Эти договоренности входят составной частью в Соглашения об Уровне Сервиса. Приведенная ниже формула помогает определить, отвечает ли достигнутый Уровень Доступности согласованным требованиям:

$$\% \text{ доступности} = \frac{\text{Достигнутое время работоспособности}}{\text{Согласованное время работоспособности}} \times 100 \%$$

Рис. 14.6. Формула доступности (источник: OGC)

Достигнутое время работоспособности системы равно разнице между согласованным временем работоспособности и случившемся временем простоя. Например: если была достигнута договоренность о 98% доступности сервиса в рабочие дни с 7.00 до 19.00 и в течение это периода был двухчасовой отказ сервиса, то достигнутое время работоспособности (процент доступности) будет равен:

$$(5 \times 12 - 2) / (5 \times 12) \times 100\% = 96,7\%$$

¹ CCTA Risk Analysis and Management Method - CRAMM.

Анализ простоев системы¹ (SOA)

Данный метод можно использовать для выяснения причин сбоев, изучения эффективности ИТ-организации и ее процессов, а также для представления и реализации предложений по усовершенствованию сервиса.

Характеристики метода SOA:

- широкая сфера действия: он не ограничивается инфраструктурой и охватывает также процессы, процедуры и аспекты корпоративной культуры;
- рассмотрение вопросов с точки зрения заказчика;
- совместная реализация метода представителями заказчика и ИТ-организации (команда метода SOA).

К числу преимуществ данного метода относятся эффективность подхода, прямая связь между заказчиком и поставщиком и более широкая область для предложений по улучшению сервиса.

Пост технического наблюдения² (ТОР)

Данный метод заключается в наблюдении специальной командой ИТ-специалистов одного выбранного аспекта доступности. Его можно использовать в тех случаях, когда обычные средства не обеспечивают достаточной поддержки. Метод ТОР позволяет объединить знания проектировщиков и руководителей систем.

Основным достоинством данного метода является рациональный, эффективный и неформальный подход, который быстро дает результат.

14.5. Контроль процесса

14.5.1. Составление отчетов

Составление отчетов о доступности сервиса для заказчика обсуждалось выше. Для целей контроля процесса можно использовать следующие метрики:

- время обнаружения;
- время реагирования;
- время ремонта;
- время восстановления;
- оценка успешности использования соответствующих методов (CFIA, CRAMM, SOA);
- степень реализации процесса: услуги, Соглашения об Уровне Сервиса и группы заказчиков, попадающие под действия Соглашения об Уровне Сервиса.

Некоторые метрики можно задать для каждой услуги, команды или области инфраструктуры (сети, вычислительного центра и рабочей станции).

14.5.2. Критические факторы успеха и ключевые показатели эффективности

Критическими факторами успеха Процессы Управления Доступностью сервиса являются:

- наличие у бизнеса четко определенных целей и пожеланий в отношении доступности сервиса;
- налаженный Процесс Управления Уровнем Сервиса для обеспечения формализации соглашений;
- одинаковое понимание сторонами понятий доступности и простоя;

¹ System Outage Analysis — SOA.

² Technical Observation Post - TOR

- понимание как бизнесом, так и ИТ-организацией преимуществ Управления Доступностью.

Об эффективности и рациональности Процесса Управления Доступностью свидетельствуют такие показатели эффективности, как:

- доступность сервиса в процентном выражении (время работоспособности) в проекции услуг или
 - групп пользователей;
 - продолжительность простоев;
 - частота возникновения простоев.

14.5.3. Функции и роли

В организации может быть назначена роль Руководителя Процесса Управления Доступностью для того, чтобы планировать и поддерживать процесс. Задача Руководителя процесса состоит в следующем:

- определение (формирование) процесса и его разработка в организации;
- обеспечение разработки ИТ-сервисов, при которой достигнутые Уровни Сервиса (в Плате Доступности, Надежности, Обслуживания и Способности к Восстановлению) будут соответствовать согласованным уровням;
- составление отчетов;
- оптимизация доступности ИТ-инфраструктуры с целью обеспечения рентабельного улучшения сервиса, предоставляемого бизнесу.

14.6. Проблемы и затраты

14.6.1. Проблемы

Большинство проблем данного процесса связано с организационными вопросами. Среди возможных проблем могут быть следующие:

- руководство распределяет ответственность за доступность сервисов по нескольким направлениям — между линейными руководителями, руководителями процессов. Каждый руководитель отвечает за свое направление, что приводит к отсутствию общей координации;
- ИТ-руководство не понимает той добавочной стоимости, которую дают Процессы Управления Инцидентами, Проблемами и Изменениями;
- существующий Уровень Доступности считается достаточным
- отсутствует понимание необходимости назначения одного руководителя, несущего ответственность за процесс;
- у руководителя процесса нет достаточных полномочий.

Даже если имеется достаточная поддержка со стороны руководства, проблемы все равно могут возникать по следующим причинам:

- недооценка необходимых ресурсов;
- недостаток эффективных инструментальных средств измерения и составления отчетов;
- недостаточный Уровень Зрелости других процессов, таких как Управление Уровнем Сервиса, Управление Конфигурациями и Управление Проблемами.

Эти проблемы решаемы при должной поддержке со стороны ИТ-руководства, опытным руководителем процесса, несущего за него полную ответственность, при наличии необходимых инструментальных средств, быстром и эффективном разрешении имеющихся проблем.

При нерациональном использовании Процесса Управления Доступностью могут возникнуть следующие проблемы:

- трудности при определении соответствующих стандартов доступности;
- трудности в руководстве и координации внешних и внутренних поставщиков;
- трудности при определении и сравнении стоимости доступности и недоступности;
- если стандарты доступности не учитывались на этапе проектирования, то последующие модификации, выполняемые с целью достижения соответствия стандартам, могут оказаться очень дорогостоящими;
- несоответствие стандартам доступности может привести к невозможности достижения поставленных бизнес-целей;
- может понизиться Уровень Удовлетворенности Заказчика.

Другой потенциальной проблемой является нацеленность на сверхвысокую доступность сервиса. В этом случае резко возросшие затраты не будут окупаться полученными преимуществами. Все же всегда имеется вероятность возникновения простоя. Процесс Управления Доступностью играет важную роль в разрешении таких нежелательных ситуаций.

14.6.2. Затраты

Затраты на процесс состоят из:

- затрат на внедрение процесса;
- затрат на персонал;
- затрат на устройства;
- затрат на инструментальные средства измерения и составления отчетов.

Для улучшения показателей доступности необходимо уже на ранних этапах определить необходимый Уровень Инвестиции в этот процесс. Всегда должен выполняться анализ рентабельности, так как обычно улучшение доступности связано с ростом затрат. Найти оптимальное решение этой проблемы — важная задача Процесса Управления Доступностью. Как показывает опыт, оптимальное решение можно найти, используя разумные ресурсы без крупных дополнительных инвестиций.

При обсуждении стоимости и преимуществ внедрения процесса следует руководствоваться тем, какими могли бы быть затраты, если полностью игнорировать Процесс Управления Доступностью и оказаться в ситуации, когда не будут выполнены согласованные требования по доступности сервиса. Такая ситуация может иметь следующие последствия для заказчика:

- снижение производительности;
- уменьшение оборота бизнеса и прибыли;
- затраты на восстановление;
- возможные претензии третьих сторон и т. д.

Перечисленные ниже аспекты трудно представить в количественном выражении, тем не менее они очень важны:

- потеря престижа и заказчиков;
- потеря репутации и доверия;
- потеря мотивации персонала и удовлетворенности работой.

Процесс Управления Доступностью может помочь ИТ-организации избежать этих потерь и достичь поставленных целей путем предоставления заказчикам необходимых услуг по приемлемой и обоснованной цене.

Глава 15

Управление Информационной Безопасностью

15.1. Введение

Существование многих бизнес-процессов невозможно без информационного обеспечения. Фактически все больше и больше бизнес-процессов состоят исключительно из одной или нескольких информационных систем. Управление Информационной Безопасностью — важный вид деятельности, целью которого является контроль процессов обеспечения информацией и предотвращение ее несанкционированного использования.

В течение многих лет проблемы Управления Информационной Безопасностью в значительной степени игнорировались. Ситуация меняется. Безопасность сейчас считается одной из главных проблем менеджмента на предстоящие годы. Интерес к этому предмету повышается из-за растущего использования сети Интернет и особенно электронной коммерции. Все больше видов бизнеса открывают электронные шлюзы к своей деятельности. Это вызывает опасность постороннего вмешательства и поднимает некоторые важные для бизнеса вопросы. Какие риски мы хотим контролировать и какие меры мы должны предпринять сейчас и в течение следующего бюджетного цикла? Руководство высшего уровня должно принимать решения, а это возможно только при глубоком анализе рисков. Этот анализ должен предоставить входную информацию для Процесса Управления Информационной Безопасностью, необходимую для определения требований безопасности.

Требования бизнеса к информационной безопасности оказывают воздействие на поставщиков ИТ-услуг и должны быть заложены в Соглашениях об Уровне Сервиса. Задачей Процесса Управления Информационной Безопасностью является постоянное обеспечение безопасности услуг на согласованном с заказчиком уровне. Безопасность в настоящее время является важнейшим показателем качества менеджмента.

Процесс Управления Информационной Безопасностью способствует интеграции аспектов безопасности в ИТ-организацию с точки зрения поставщика услуг. Сборник практических рекомендаций по Управлению Информационной Безопасностью (BS 7799) дает руководство для разработки, введения и оценки мер безопасности.

15.1.1. Основные понятия

Процесс Управления Информационной Безопасностью входит в сферу компетенции общей информационной безопасности, задачей которой является обеспечение сохранности информации. Сохранность означает защищенность от известных рисков и, по возможности, уклонение от неизвестных рисков. Инструментом обеспечения этого является безопасность. Целью является защита ценной информации. Ценность информации влияет на необходимый Уровень Конфиденциальности, целостности и доступности.

- **Конфиденциальность** — защита информации от несанкционированного доступа и использования.
- **Целостность** — точность, полнота и своевременность информации.
- **Доступность** — информация должна быть доступна в любой момент предварительного согласованного временного интервала. Это зависит от *непрерывности* работы систем обработки информации.

Вторичные аспекты включают приватность (конфиденциальность и целостность частной информации), анонимность и проверяемость (возможность проверки правильного использования информации и эффективности мер безопасности).

15.2. Цели процесса

В последние десятилетия почти все виды бизнеса стали более зависимыми от информационных систем. Использование компьютерных сетей также возросло, они не

ограничиваются рамками одной организации, они соединяют бизнес-партнеров и обеспечивают связь с внешним миром. Возрастающая сложность ИТ-инфраструктуры означает, что бизнес становится более уязвимым по отношению к техническим сбоям, человеческим ошибкам, злоумышленным действиям, хакерам и взломщикам, компьютерным вирусам и т. д. Эта растущая сложность требует унифицированного управленческого подхода. Процесс Управления Информационной Безопасностью имеет важные связи с другими процессами. Некоторые виды деятельности по обеспечению безопасности осуществляются другими процессами библиотеки ITIL, под контролем Процесса Управления Информационной Безопасностью.

Процесс Управления Информационной Безопасностью имеет две цели:

- выполнение требований безопасности, закрепленных в SLA и других требованиях внешних договоров, законодательных актов и установленных правил;
- обеспечение базового Уровня Безопасности, независимого от внешних требований.

Процесс Управления Информационной Безопасностью необходим для поддержки непрерывного функционирования ИТ-организации. Он также способствует упрощению Управления Информационной Безопасностью в рамках Управления Уровнями Сервиса, так как степень сложности Управления SLA зависит также от их количества.

Входными данными для процесса служат соглашения SLA, определяющие требования безопасности, по возможности дополненные документами, определяющими политику компании в этой области, а также другие внешние требования. Процесс также получает важную информацию, относящуюся к проблемам безопасности из других процессов, например об инцидентах, связанных с безопасностью. Выходные данные включают информацию о достигнутой реализации соглашений SLA вместе с отчетами о нештатных ситуациях с точки зрения безопасности и регулярные Планы по безопасности. В настоящее время многие организации имеют дело с информационной безопасностью на стратегическом уровне — в информационной политике и информационном планировании, и на операционном уровне, при закупке инструментария и других продуктов обеспечения безопасности. Недостаточно внимания уделяется реальному Управлению Информационной Безопасностью, непрерывному анализу и преобразованию правил работы в технические решения, поддержанию эффективности мер безопасности при изменении требований и среды. Следствием разрыва между операционным и стратегическим уровнями является то, что на тактическом уровне значительные средства вкладываются в уже неактуальные меры безопасности, в то время как должны быть приняты новые, более эффективные меры. Задачей Процесса Управления Информационной Безопасностью является обеспечение принятия эффективных мер по информационной безопасности на стратегическом, тактическом и операционном уровнях.

15.2.1. Преимущества использования процесса

Информационная безопасность не является самоцелью; она должна служить интересам бизнеса и организации. Некоторые виды информации и информационных услуг являются для организации более важными, чем другие. Информационная безопасность должна соответствовать Уровню Важности Информации. Безопасность планируется путем соблюдения баланса между мерами безопасности, ценностью информации и существующими угрозами в среде обработки. Эффективное информационное обеспечение с адекватной защитой информации важно для организации по двум причинам:

- **Внутренние причины:** эффективное функционирование организации возможно только при наличии доступа к точной и полной информации. Уровень Информационной Безопасности должен соответствовать этому принципу.

- **Внешние причины:** в результате выполнения в организации определенных процессов создаются продукты и услуги, которые доступны для рынка или общества, для выполнения определенных задач. Неадекватное информационное обеспечение ведет к производству некачественных продуктов и услуг, которые не могут использоваться для выполнения соответствующих задач и ставят под угрозу существование организации. Адекватная защита

информации является важным условием для адекватного информационного обеспечения. Таким образом внешнее значение информационной безопасности определяется отчасти ее внутренним значением.

Безопасность может создавать значительную добавочную стоимость для информационных систем. Эффективная безопасность способствует непрерывности функционирования организации и выполнению ее целей.

15.3. Процесс

Организации и их информационные системы меняются. Стандартные шаблоны, такие как Сборник практических рекомендаций по Управлению Информационной Безопасностью (Code of Practice for Information Security Management), статичны и недостаточно соответствуют быстрым изменениям в ИТ. По этой причине деятельность, ведущаяся в рамках Процесса Управления Информационной Безопасностью, должна постоянно пересматриваться в целях обеспечения эффективности Процесса. Управление Информационной Безопасностью сводится к никогда не прекращающемуся циклу планов, действий, проверок и актов. Виды деятельности, проводимые в рамках процесса Управления Информационной Безопасностью или в других процессах под контролем Управления Информационной Безопасностью, описываются ниже.

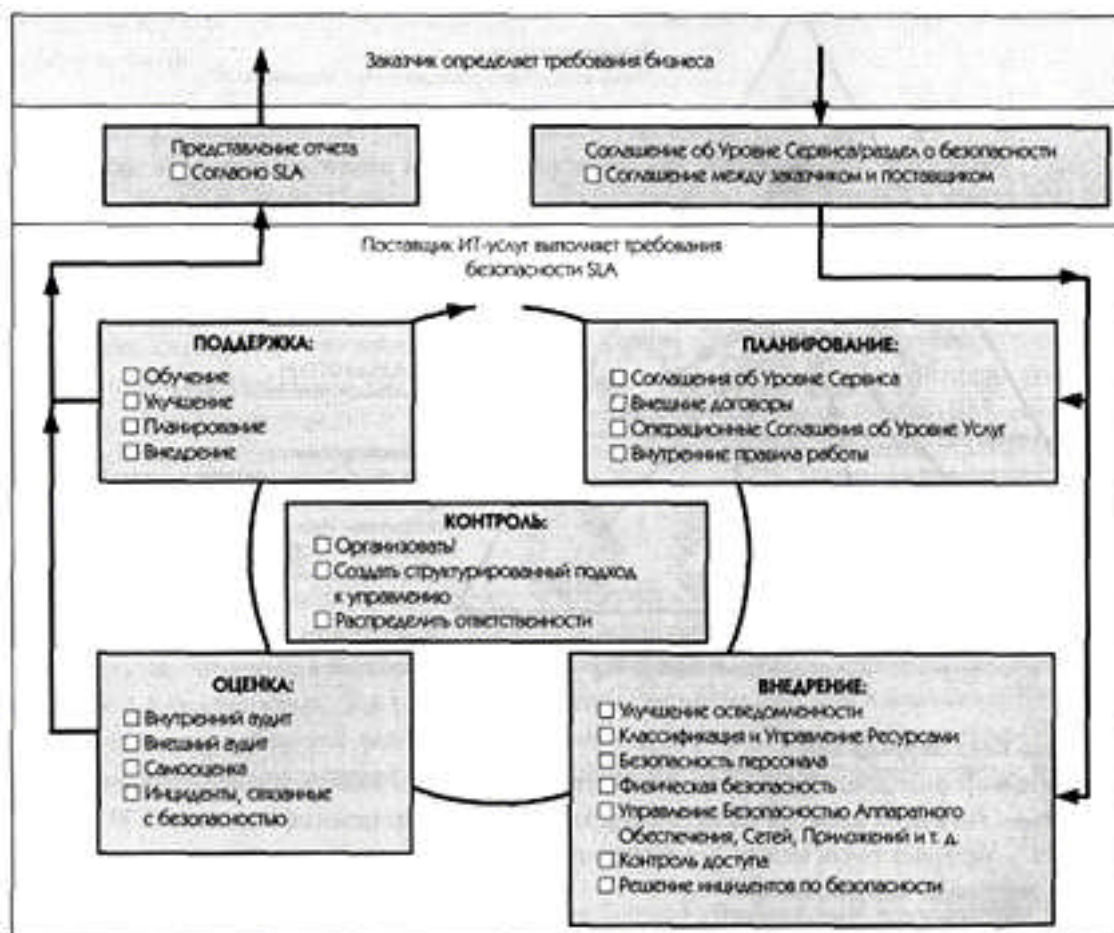


Рис. 15.1. Процесс Управления Информационной Безопасностью (источник: OGC)

Требования заказчика изображены в правом верхнем углу, как входные данные процесса. Эти требования определяются в разделе о безопасности Соглашения об Уровне Сервиса как услуги по безопасности и обеспечиваемый Уровень Безопасности. Поставщик услуг доводит эти соглашения до ИТ-организации в форме Плана по безопасности, определяющего критерии безопасности или операционные Соглашения об Уровне Услуг. Этот план выполняется и результаты оцениваются. Затем план и способы его реализации корректируются, о чем Управление Уровнем Сервиса сообщает заказчику. Таким образом, заказчик и поставщик услуг вместе участвуют в формировании всего цикла процесса. Заказчик может изменить требования

на основе получаемых отчетов, а поставщик услуг может скорректировать план или его реализацию на основе результатов наблюдения или поставить задачу изменения договоренностей, определенных в соглашении SLA. Функция контроля представлена в центре рисунка 15.1. Далее эта диаграмма будет использоваться при описании видов деятельности Процесса Управления Информационной Безопасностью.

15.3.1. Взаимоотношения с другими процессами

Процесс Управления Информационной Безопасностью имеет связи с другими процессами ITIL (см. рис. 15.2), так как в других процессах выполняются действия, связанные с обеспечением безопасности. Эта деятельность проводится в обычном порядке в рамках ответственности определенного процесса и его руководителя. При этом Процесс Управления Информационной Безопасностью обеспечивает другие процессы инструкциями о структуре деятельности, связанной с безопасностью. Обычно соглашения об этом определяются после консультаций между Руководителем Процесса Управления Информационной Безопасностью и Руководителями других процессов.

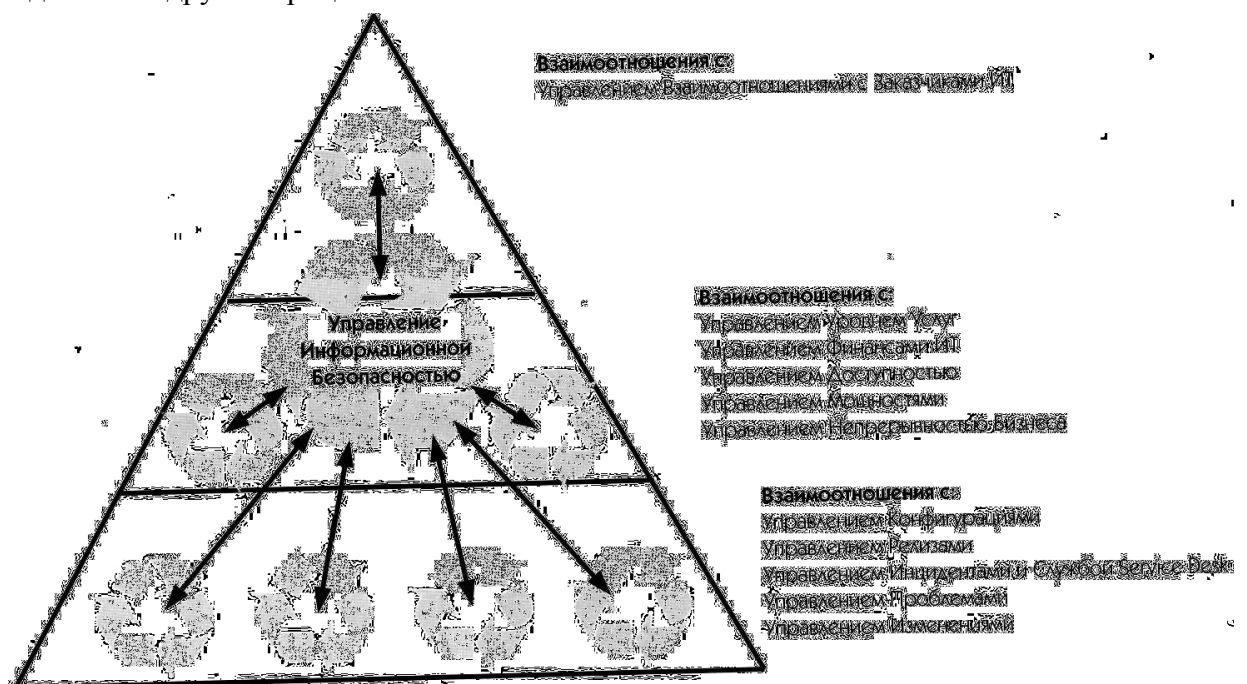


Рис. 15.2. Отношения между Процессом Управления Информационной Безопасностью и другими процессами (источник: OGC)

Управление Конфигурациями

В контексте информационной безопасности процесс Управления Конфигурациями имеет наибольшее значение, так как он позволяет классифицировать Конфигурационные Единицы (CI). Эта классификация определяет связи между Конфигурационными Единицами и предпринимаемыми мерами или процедурами безопасности.

Классификация Конфигурационных Единиц определяет их конфиденциальность, целостность и доступность. Эта классификация основана на требованиях безопасности соглашений SLA. Заказчик ИТ-организации определяет классификацию, так как только заказчик может решить, насколько важны информация или информационные системы для бизнес-процессов. При создании классификации Конфигурационных Единиц заказчик учитывает степень зависимости бизнес-процессов от информационных систем и информации. Затем ИТ-организация увязывает классификацию с соответствующими Конфигурационными Единицами. ИТ-организация должна также реализовать комплекс мер безопасности для каждого Уровня Классификации. Эти комплексы мер могут быть описаны как процедуры, например «Процедура обращения с носителями данных с личной информацией». В соглашении SLA могут определяться комплексы мер безопасности для каждого Уровня Классификации. Система

классификации должна всегда быть совместима со структурой организации заказчика. Однако для упрощения управления рекомендуется использовать одну общую систему классификации, даже если ИТ-организация имеет несколько заказчиков.

Из вышесказанного можно сделать вывод, что классификация является ключевым моментом. Каждая Конфигурационная Единица в Конфигурационной Базе Данных (CMDB) должна быть классифицирована. Эта классификация связывает Конфигурационную Единицу с соответствующим комплексом мер безопасности или процедурой.

Управление Инцидентами

Управление Инцидентами является важным процессом, информирующим о наличии инцидентов, связанных с безопасностью. По своей природе связанные с безопасностью инциденты могут быть обработаны с помощью иной процедуры, чем другие инциденты. Поэтому важно, чтобы Процесс Управления Инцидентами распознавал инциденты по безопасности как таковые. Любой инцидент, который может помешать выполнению требований безопасности SLA, классифицируется как инцидент по безопасности. Было бы полезным включить в соглашения SLA определение типов инцидентов, рассматривающихся как инциденты по безопасности. Любой инцидент, препятствующий достижению базового внутреннего Уровня Безопасности, также всегда классифицируется как инцидент по безопасности.

Сообщения об инцидентах поступают не только от пользователей, но также от различных Процессов Управления, возможно, на основе аварийных сигналов или данных системного аудита. Крайне необходимо, чтобы Процесс Управления Инцидентами распознавал все инциденты по безопасности. Это требуется для инициирования соответствующих процедур для обработки таких инцидентов. Рекомендуется включить в планы процедуры для различных типов инцидентов по безопасности и опробовать их на практике. Также рекомендуется согласовывать процедуру оповещения об инцидентах, связанных с безопасностью. Нередко паника возникает из-за чрезмерно раздутых слухов. Точно так же нередко отсутствие своевременного оповещения об инцидентах по безопасности приводит к возникновению ущерба. Желательно, чтобы все внешние сообщения, относящиеся к инцидентам по безопасности, проходили через руководителя Процесса Управления Информационной Безопасностью.

Управление Проблемами

Процесс Управления Проблемами отвечает за идентификацию и устранение структурных сбоев по безопасности. Проблема может также привести к возникновению риска для системы безопасности. В этом случае Управление Проблемами должно привлечь на помощь Процесс Управления Информационной Безопасностью. Для того чтобы не возникло новых проблем с безопасностью, принятое окончательное или обходное решение должно быть проверено. Эта проверка должна основываться на соответствии предлагаемых решений требованиям соглашений SLA и внутренним требованиям безопасности.

Управление Изменениями

Виды работ, выполняемых в рамках Процесса Управления Изменениями, часто бывают тесно связаны с безопасностью, так как Управление Изменениями и Управление Информационной Безопасностью взаимозависимы. Если достигнут приемлемый Уровень Безопасности, который находится под контролем Процесса Управления Изменениями, то можно гарантировать, что этот Уровень Безопасности будет обеспечиваться и после проведения изменений. Для поддержки этого Уровня Безопасности существует ряд стандартных операций. Каждый Запрос на изменения (RFC) связан с рядом параметров, которые определяют процедуру приемки. Параметры срочности и степени воздействия могут быть дополнены параметром, связанным с безопасностью. Если Запрос на изменения (RFC) может оказать значительное воздействие на информационную безопасность, потребуются расширенные приемочные испытания и процедуры.

В Запрос на изменения (RFC) также должны быть включены предложения по решению вопросов безопасности. Они опять же должны основываться на требованиях SLA и базовом Уровне Внутренней Безопасности, необходимом для ИТ-организации. Следовательно, эти предложения будут включать комплекс мер по обеспечению безопасности, основанный на Практических нормах по Управлению Информационной Безопасностью.

Желательно, чтобы руководитель Процесса Управления Информационной Безопасностью (а также, возможно, инспектор по безопасности от заказчика) был членом Консультативного комитета по изменениям (Change Advisory Board — CAB).

Однако это не значит, что по всем изменениям необходимо консультироваться с Руководителем Процесса Управления Информационной Безопасностью. В нормальной ситуации безопасность должна быть интегрирована в обычный рабочий режим. Руководитель Процесса Управления Изменениями должен иметь возможность решать, требуется ли ему или комитету CAB входная информация от Руководителя Процесса Управления Информационной Безопасностью. Точно так же руководитель Процесса Управления Информационной Безопасностью не обязательно должен участвовать в выборе мер для конкретных Конфигурационных Единиц затронутых Запросом на Изменения (RFC), так как для соответствующих мер уже должен существовать структурированный подход. Вопросы могут возникнуть только со способом реализации указанных мер.

Любые меры безопасности, связанные со внесением изменений, должны реализовываться одновременно с проведением самих изменений, и они должны тестироваться совместно. Тесты безопасности отличаются от обычных функциональных тестов. Задачей обычных тестов является определение доступности определенных функций. При тестировании безопасности проверяют не только доступность функций безопасности, но также отсутствие других, нежелательных функций, которые могут снизить безопасность системы.

С точки зрения безопасности Управление Изменениями является одним из наиболее важных процессов. Это объясняется тем, что Управление Изменениями вводит новые меры безопасности в ИТ-инфраструктуру вместе с изменениями этой инфраструктуры.

Управление Релизами

Процесс Управления Релизами осуществляет контроль и развертывание всех новых версий программного и аппаратного обеспечения, оборудования для передачи данных и т. д. Этот процесс гарантирует, что:

- используется соответствующее аппаратное и программное обеспечение;
- аппаратное и программное обеспечение тестируются перед использованием;
- внедрение надлежащим образом санкционировано с помощью процедуры изменения;
- программное обеспечение является легальным;
- программное обеспечение не содержит вирусов, и вирусы не появятся при его распространении;
- номера версий известны и зарегистрированы в Базе Данных CMDB Процессом Управления Конфигурациями;
- управление развертыванием будет эффективным.

В этом процессе также используется обычная процедура приемки, которая должна охватывать аспекты информационной безопасности. Рассмотрение аспектов безопасности во время тестирования и приемки является особенно важным. Это означает, что требования и меры по безопасности, определенные в SLA, должны соблюдаться постоянно.

Управление Уровнем Сервиса

Процесс Управления Уровнем Сервиса гарантирует, что договоренности об услугах, предоставляемых заказчиком, определены и выполняются. В Соглашениях об Уровне Сервиса должны учитываться также меры безопасности. Целью этого является оптимизация Уровня

Предоставляемых Услуг. Управление Уровнем Сервиса включает ряд видов деятельности, связанных с безопасностью, в которых важную роль играет Управление Информационной Безопасностью:

1. Определение потребностей заказчика в области безопасности. Естественно, определение необходимости в безопасности является ответственностью заказчика, так как эти потребности основаны на его интересах.
2. Проверка осуществимости требований заказчика по безопасности.
3. Предложение, обсуждение и определение Уровня Безопасности ИТ-услуг в SLA.
4. Определение, разработка и формулирование внутренних требований безопасности для ИТ-услуг (Операционные Соглашения об Уровне Услуг — OLA).
5. Мониторинг стандартов безопасности (OLA).
6. Составление отчетов о предоставляемых услугах.

Управление Информационной Безопасностью предоставляет Управлению Уровнем Сервиса входную информацию и поддержку для осуществления видов деятельности с 1 по 3. Виды деятельности 4 и 5 проводятся Управлением Информационной Безопасностью. Для деятельности 6 Управление Информационной Безопасностью и другие процессы предоставляют необходимую входную информацию. Руководители Процессов Управления Уровнем Сервиса и Управления Информационной Безопасностью после взаимных консультаций решают, кто реально занимается проведением этих операций. При составлении соглашений SLA обычно предполагается, что существует общий базовый Уровень Безопасности (baseline). Дополнительные требования заказчика по безопасности должны четко определяться в SLA.

Управление Доступностью

Процесс Управления Доступностью рассматривает техническую доступность ИТ-компонентов, связанную с доступностью услуги. Качество доступности определяется непрерывностью, ремонтпригодностью и устойчивостью. Так как многие меры безопасности оказывают положительное воздействие и на доступность, и на аспекты безопасности — конфиденциальность и целостность, существенно важной является координация мер между Процессами Управления Доступностью, Управления Непрерывностью ИТ-услуг и Управления Информационной Безопасностью.

Управление Мощностями

Процесс Управления Мощностями отвечает за наилучшее использование ИТ-ресурсов в соответствии с договоренностью с заказчиком. Требования по производительности основаны на количественных и качественных стандартах, определенных Управлением Уровнем Услуг. Почти все виды деятельности Процесса Управления Мощностями воздействуют на доступность и, следовательно, также на Процесс Управления Информационной Безопасностью.

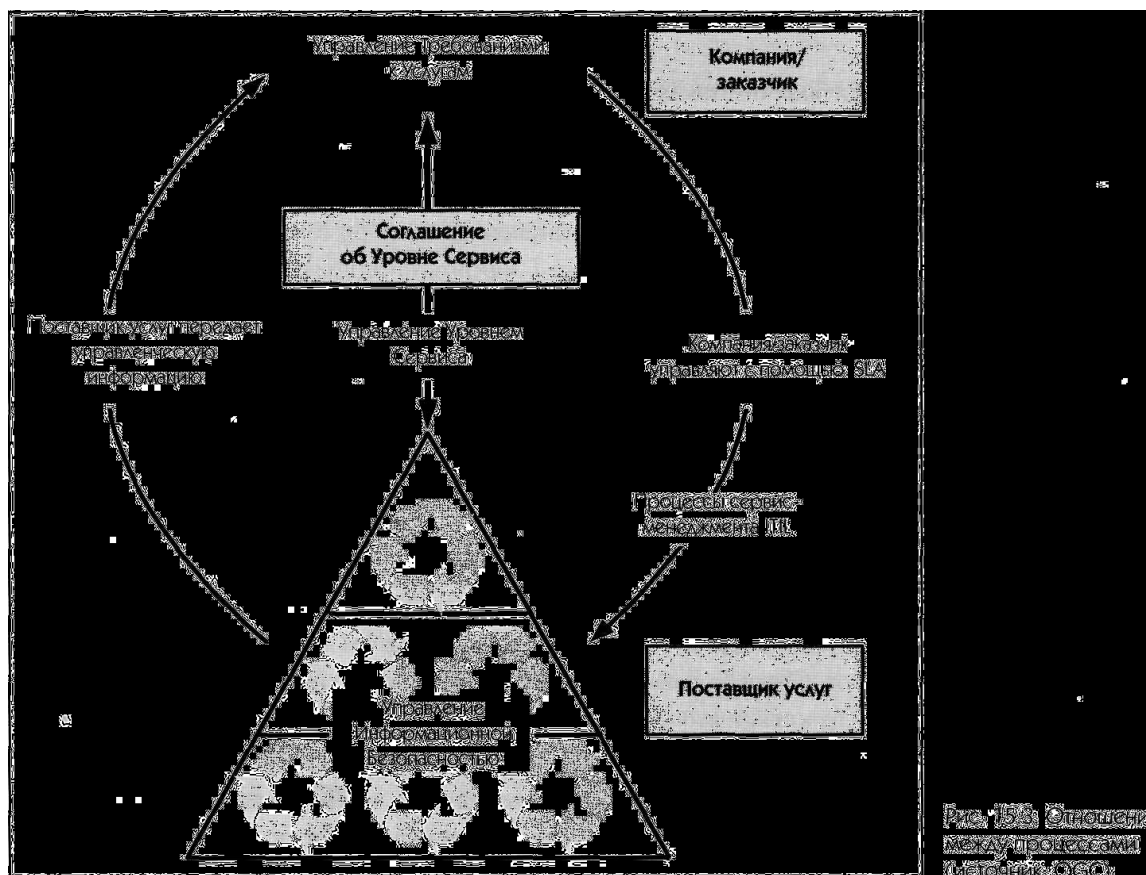
Управление Непрерывностью ИТ-услуг

Процесс Управления Непрерывностью ИТ-услуг гарантирует, что воздействие любых непредвиденных обстоятельств будет ограничиваться уровнем, согласованным с заказчиком. Чрезвычайные обстоятельства не обязательно должны превращаться в катастрофы. Основными видами деятельности являются определение, поддержка, внедрение и тестирование плана обеспечения непрерывной работы и восстановления функционирования, а также принятие превентивных мер. Из-за присутствия в этих видах работ аспектов безопасности возникает связь с Процессом Управления Информационной Безопасностью. С другой стороны, невозможность выполнения базовых требований безопасности может сама рассматриваться как чрезвычайное обстоятельство.

15.3.2. Раздел по Безопасности Соглашения об Уровне Сервиса

Соглашение об Уровне Сервиса (SLA) определяет договоренности с заказчиком. Процесс Управления Уровнем Сервиса отвечает за соглашения SLA (см. также главу 10). Соглашение SLA является главной движущей силой всех процессов ITIL.

ИТ-организация определяет степень выполнения требований SLA, включая требования по безопасности. Определенные в SLA элементы безопасности должны отвечать соответствующим потребностям заказчика. Заказчик должен определить важность всех бизнес-процессов (см. рис. 15.3).



Эти бизнес-процессы зависят от ИТ-услуг, а поэтому и от ИТ-организации. Заказчик определяет требования к безопасности (требования к информационной безопасности SLA на рис. 15.3 отсутствуют) на основе анализа риска. На рис. 15.4 показано, как определяются элементы безопасности SLA.



Элементы безопасности обсуждаются представителями заказчика и поставщика услуг. Поставщик услуг сравнивает требования к Уровню Услуг Заказчика со своим Каталогом Услуг,

где описываются стандартные меры безопасности (базовый Уровень Безопасности). Заказчик может выдвигать дополнительные требования.

Заказчик и поставщик сравнивают требования по Уровню Услуг с Каталогом Услуг. В разделе соглашения SLA по безопасности могут рассматриваться такие вопросы, как общая политика информационной безопасности, список авторизованного персонала, процедуры защиты ресурсов, ограничения на копирование данных и т. д.

15.3.3. Раздел по Безопасности Операционного Соглашения об Уровне Услуг (OLA)

Еще одним важным документом является Операционное Соглашение об Уровне Услуг. В нем описываются услуги, предоставляемые внутренним поставщиком услуг. Поставщик должен связать эти договоренности с видами ответственности, существующими внутри организации. В Каталоге Услуг дается их общее описание. В Операционном Соглашении об Уровне Услуг эти общие описания преобразуются в конкретные определения всех услуг и их компонентов, а также способа выполнения договоренностей об Уровнях Услуг внутри организации.

Пример. В Каталоге Услуг значится «управление авторизацией пользователей и частных лиц». Операционное Соглашение об Уровне Услуг конкретизирует это для всех определенных услуг, предоставляемых ИТ-организацией. Таким образом реализация мероприятия определяется для подразделений, предоставляющих услуги UNIX, VMS, NT, Oracle и т. д.

Там, где это возможно, требования заказчика к Уровню Сервиса определяются по Каталогу Услуг, а в случае необходимости заключаются дополнительные соглашения. Такие дополнительные меры повышают Уровень Безопасности по сравнению со стандартным.

При составлении соглашения SLA необходимо согласовывать с Управлением Информационной Безопасностью измеряемые Ключевые показатели эффективности (KPI) и критерии. Показатели эффективности должны быть измеряемыми параметрами (метриками), а критерии эффективности должны устанавливаться на достижимом уровне. В некоторых случаях бывает трудно достичь договоренности по измеряемым параметрам безопасности. Их легче определить для доступности сервиса, которая может иметь цифровое выражение. Однако для целостности и конфиденциальности сделать это значительно труднее. Поэтому в разделе по безопасности в соглашении SLA необходимые меры обычно описываются абстрактным языком. Практические нормы по Управлению Информационной Безопасностью используются как базовый комплекс мер безопасности. В соглашении SLA также описывается метод определения эффективности. ИТ-организация (поставщик услуг) должна регулярно предоставлять отчеты организации пользователя (заказчика).

15.4. Виды деятельности

15.4.1. Контроль- политика и организация информационной безопасности

Контроль информационной безопасности, представленный в центре рисунка 15.1, является первым подпроцессом Управления Информационной Безопасностью, и относится к организации и Управлению Процессом. Этот вид деятельности включает в себя структурированный подход Управления Информационной Безопасностью, который описывает следующие подпроцессы: формулирование Планов по безопасности, их реализация, оценка реализации и включение оценки в годовые Планы по безопасности (планы действий). Также описываются отчеты, предоставляемые заказчику через Процесс Управления Уровнем Сервиса.

Этот вид деятельности определяет подпроцессы, функции безопасности, роли и ответственности. Он также описывает организационную структуру, систему отчетности и потоки управления (кто кого инструктирует, кто что делает, как производится доклад о выполнении). Следующие меры из сборника практических рекомендаций по Управлению Информационной Безопасностью реализуются в рамках этого вида деятельности.

Внутренние правила работы (политика)¹:

• разработка и реализация внутренних правил работы (политики), связи с другими правилами;

- цели, общие принципы и значимость;
- описание подпроцессов;
- распределение функций и ответственностей по подпроцессам;
- связи с другими процессами ИТIL и их управлением;
- общая ответственность персонала;
- обработка инцидентов, связанных с безопасностью.

Организация информационной безопасности:

- структурная схема управления²;
- структура управления (организационная структура);
- более детальное распределение ответственностей;
- учреждение Руководящего комитета по информационной безопасности³;
- координация информационной безопасности;
- согласование инструментальных средств (например, для анализа риска и улучшения осведомленности);
- описание процесса авторизации средств ИТ в консультации с заказчиком;
- консультации специалистов;
- сотрудничество между организациями, внутреннее и внешнее взаимодействие;
- независимый аудит информационных систем;
- принципы безопасности при доступе к информации третьих сторон;
- информационная безопасность в договорах с третьими сторонами.

15.4.2. Планирование

Подпроцесс планирования сводится к определению содержания раздела соглашений SLA по вопросам безопасности при участии Процесса Управления Уровнем Сервиса и описанию деятельности, связанной с вопросами безопасности, проводимой в рамках Внешних Договоров. Задачи, которые в соглашении SLA определяются общими словами, детализируются и конкретизируются в форме Операционного Соглашения об Уровне Услуг (OLA). Соглашение OLA может рассматриваться как План по безопасности для организационной структуры поставщика услуг и как конкретный План по безопасности, например, для каждой ИТ-платформы, приложения и сети.

Входной информацией для подпроцесса планирования являются не только положения соглашения SLA, но и принципы политики безопасности поставщика услуг (из подпроцесса контроля). Примерами этих принципов: «Каждый пользователь должен быть идентифицирован уникальным образом»; «Базовый Уровень Безопасности предоставляется всегда и для всех заказчиков».

Операционные Соглашения об Уровне Услуг (OLA) в отношении информационной безопасности (конкретные Планы по безопасности) разрабатываются и реализуются с помощью обычных процедур. Это означает, что если эти виды деятельности стали необходимы в других процессах, то нужна координация с этими процессами. Все необходимые изменения ИТ-инфраструктуры проводятся Процессом Управления Изменениями с использованием входной информации, предоставляемой Процессом Управления Информационной Безопасностью. Ответственным за Процесс Управления Изменениями является Руководитель этого Процесса.

¹ Policy.

² Management framework.

³ Information Security Steering Committee.

Подпроцесс планирования координируется с Процессом Управления Уровнем Сервиса по вопросам определения содержания раздела по безопасности соглашения SLA, его обновления и обеспечения соответствия его положениям. За эту координацию отвечает руководитель Процесса Управления Уровнем Сервиса.

Требования по безопасности должны определяться в соглашении SLA, по возможности в измеримых показателях. Раздел по безопасности соглашения SLA должен гарантировать, что достижение всех требований и стандартов безопасности заказчика может быть проконтролировано.

15.4.3. Реализация

Задачей подпроцесса реализации (внедрения) является выполнение всех мероприятий, определенных в планах. Этот подпроцесс может поддерживаться следующим контрольным списком действий.

Классификация и Управление ИТ-ресурсами:

- предоставление входных данных для поддержки Конфигурационных Единиц (CI) в базе CMDB;
- классификация ИТ-ресурсов в соответствии с согласованными принципами.

Безопасность персонала:

- задачи и ответственности в описании работ;
- отбор персонала;
- соглашения о конфиденциальности для персонала;
- обучение персонала;
- руководства для персонала по разрешению инцидентов, связанных с безопасностью, и устранению обнаруженных дефектов защиты;
- дисциплинарные меры;
- улучшение осведомленности по вопросам безопасности.

Управление Безопасностью:

- внедрение видов ответственности и распределение обязанностей;
- письменные рабочие инструкции;
- внутренние правила;
- меры безопасности должны охватывать весь жизненный цикл систем; должны существовать руководства по безопасности для разработки систем, их тестирования, приемки, операционного использования, обслуживания и вывода из операционной среды;
- отделение среды разработки и тестирования от операционной (рабочей) среды;
- процедуры обработки инцидентов (осуществляемые Процессом Управления Инцидентами);
- использование средств восстановления;
- предоставление входной информации для Процесса Управления Изменениями;
- внедрение мер защиты от вирусов;
- внедрение методов управления для компьютеров, приложений, сетей и сетевых услуг;
- правильное обращение с носителями данных и их защита.

Контроль доступа:

- внедрение политики доступа и контроля доступа;

- поддержка привилегий доступа пользователей и приложений к сетям., сетевым услугам, компьютерам и приложениям;
- поддержка барьеров сетевой защиты (фаервол, услуги доступа по телефонной линии, мосты и маршрутизаторы);
- внедрение методов идентификации и авторизации компьютерных систем, рабочих станций и ПК в сети.

15.4.4. Оценка

Существенное значение имеет независимая оценка реализации запланированных мероприятий. Такая оценка необходима для определения эффективности, ее выполнение также требуют заказчики и третьи стороны. Результаты подпроцесса оценки могут использоваться для корректировки согласованных с заказчиком мер, а также для их реализации. По результатам оценки могут быть предложены изменения, в случае чего формулируется Запрос на изменения (RFC), направляемый в Процесс Управления Изменениями.

Существует три вида оценки:

- самостоятельная оценка: проводится в первую очередь линейными подразделениями организации;
- внутренний аудит: проводится внутренними ИТ-аудиторами;
- внешний аудит: проводится внешними ИТ-аудиторами.

В отличие от самостоятельной оценки аудит не проводится тем же персоналом, который участвует в других подпроцессах. Это необходимо для обеспечения разделения ответственностей. Аудит может проводиться отделом внутреннего аудита.

Оценка также проводится как ответное действие в случае возникновения инцидентов.

Основными видами деятельности являются:

- проверка соответствия политике безопасности и реализация Планов по безопасности;
- проведение аудита безопасности ИТ-систем;
- определение и принятие мер несоответствующего использования ИТ-ресурсов;
- проверка аспектов безопасности в других видах ИТ-аудита.

15.4.5. Поддержка

В связи с изменением рисков при изменениях в ИТ-инфраструктуре, в компании и в бизнес-процессах необходимо обеспечить должную поддержку мер безопасности. Поддержка мер безопасности включает поддержку соответствующих разделов по безопасности соглашений SLA и поддержку подробных Планов по безопасности (на Уровне Операционных Соглашений об Уровне Услуг).

Поддержание эффективного функционирования системы безопасности проводится на основе результатов подпроцесса Оценки и анализа изменений рисков. Предложения могут быть внедрены или в подпроцессе планирования, или в ходе обеспечения поддержки всего соглашения SLA. В любом случае внесенные предложения могут привести ко включению дополнительных инициатив в годовой План по безопасности. Любые изменения подлежат обработке в рамках обычного Процесса Управления Изменениями.

15.4.6. Составление отчетов

Составление отчетов является видом деятельности по предоставлению информации из других подпроцессов. Отчеты составляются для предоставления информации о достигнутых

характеристиках безопасности и для информирования заказчиков о проблемах безопасности. Вопросы предоставления отчетов обычно согласовываются с заказчиком.

Составление отчетов является важным как для заказчика, так и для поставщика услуг. Заказчики должны иметь точную информацию об эффективности работы (например, по реализации мер безопасности) и о принимаемых мерах безопасности. Заказчик также информируется о любых инцидентах, связанных с безопасностью. Ниже даются предложения по составлению отчетов.

Примеры регулярных отчетов и включаемых в них событий:

Подпроцесс планирования:

- отчеты о степени соответствия соглашению SLA и согласованным ключевым показателям качества по вопросам безопасности;
- отчеты о внешних договорах и связанных с ними проблемах;
- отчеты об Операционных Соглашениях об Уровне Услуг (внутренние Планы по безопасности) и собственных принципах безопасности поставщика (например, по базовому Уровню Безопасности);
- отчеты о годовых планах по безопасности и планах действий.

Подпроцесс внедрения:

- отчеты о состоянии дел в информационной безопасности. Сюда входят отчет о выполнении годового плана по безопасности, перечень осуществленных или намеченных мер, информация об обучении, результаты дополнительного анализа рисков и т. д.;
- перечень инцидентов, связанных с безопасностью и ответных мер, возможно, в сравнении с предыдущим отчетным периодом;
- определение тенденций возникновения инцидентов;
- состояние программы оповещения.

Подпроцесс оценки:

- отчеты об эффективности подпроцессов;
- результаты аудиторских проверок, анализа и внутренних оценок;
- предупреждения, определение новых угроз.

Специальные отчеты:

Для сообщений об определенных в соглашении SLA инцидентах, связанных с безопасностью, поставщик услуг должен иметь прямой канал связи с представителем заказчика (возможно, инспектором информационной безопасности предприятия) через Руководителей Процессов Управления Уровнем Услуг, Управления Инцидентами или Управления Информационной Безопасностью. Должна быть также определена процедура для связи в особых случаях. За исключением особых обстоятельств, отчеты передаются через Процесс Управления Уровнем Услуг.

15.5. Контроль процесса

15.5.1. Критические факторы успеха и ключевые показатели эффективности

Критическими факторами успеха являются:

- полное понимание необходимости процесса со стороны руководства и его привлечение к процессу;
- привлечение пользователей к разработке процесса;
- точное определение и разделение ответственностей.

Показатели эффективности Процесса Управления Информационной Безопасностью соответствуют таким же показателям Процесса Управления Уровнем Сервиса в той степени, в которой последние связаны с затрагиваемыми в SLA вопросами безопасности.

15.5.2. функции и роли

В небольших ИТ-организациях один человек может руководить несколькими процессами. В крупных же организациях несколько человек работают над одним процессом, например, таким как Управление Информационной Безопасностью. В таких случаях обычно назначается один руководитель Процесса Управления Информационной Безопасностью. Этот руководитель несет ответственность за эффективное функционирование процесса. Его коллегой в организации заказчика является инспектор информационной безопасности.

15.6. Проблемы и затраты

15.6.1. Проблемы

Следующие аспекты имеют существенное значение для успешной реализации Процесса Управления Информационной Безопасностью:

- **Понимание необходимости процесса (понимание со стороны участников):** меры безопасности редко встречают быстрое положительное понимание со стороны персонала; чаще встречается сопротивление, а не одобрение. Пользователи возмущаются потерей определенных привилегий из-за введения мер безопасности, даже если эти возможности не являются существенными для их работы. Это объясняется тем, что привилегии дают им определенный статус. Поэтому необходима специальная работа по мотивации пользователей и получению согласия руководства на введение мер безопасности. Особенно в области Управления Информационной Безопасностью руководство должно показать пример («разъяснять курс» и «вести за собой»). При отсутствии инцидентов по безопасности у руководства может возникнуть искушение сократить расходы на Управление Безопасностью.

- **Отношение:** информационные системы небезопасны не из-за их технического несовершенства, а из-за ошибок при использовании технологии. Обычно это связано с человеческим отношением и поведением. Это означает, что процедуры безопасности должны быть интегрированы в рутинные операции.

- **Осведомленность:** осведомленность или, скорее, коммуникации является ключевым понятием. Между коммуникациями и безопасностью иногда возникает конфликт интересов: коммуникации мостят дорогу, а безопасность создает препятствия. Это означает, что реализация мер безопасности требует использования всех способов коммуникаций для того, чтобы пользователи приняли необходимый стиль поведения.

- **Верификация:** должна существовать возможность проверки и верификации безопасности. Это относится как ко вводимым мерам, так и к причинам их введения. Необходима возможность убедиться, что в соответствующих обстоятельствах приняты правильные решения. Например, должна быть возможность проверки полномочий тех, кто принимал решения.

- **Управление Изменениями:** часто при проведении изменений ослабевает качество оценки соответствия базовому Уровню Безопасности.

- **Амбиции:** при желании организации делать все сразу часто возникают ошибки. В случае введения Процесса Управления Информационной Безопасностью реализация технических мер гораздо менее важна по сравнению с организационными мерами. Изменение организации требует поэтапного подхода и занимает длительное время.

- **Отсутствие систем обнаружения:** новые системы, такие, как Интернет, не были рассчитаны на безопасность и необходимость обнаружения взлома. Причина заключается в том, что разработка защищенной системы требует больше времени, чем незащищенной, и находится в конфликте с требованиями бизнеса по невысокой стоимости разработки и скорейшей поставке на рынок.

- **Чрезмерные надежды на технологию «неприступной крепости»:** угрозы безопасности систем все чаще возникают в непредсказуемых местах. Сравните первые атаки вирусов ILOVEYOU и Nimda с первым примером атак Denial of Service (DoS). В то время как защита информации с использованием традиционного подхода «неприступной крепости» сохраняет свое значение, также приобретает важность подхода «встречных атак» при возникновении нарушений безопасности. Организация должна иметь возможность быстро направить ресурсы в место возникновения дефекта до того, как он сможет выйти из-под контроля.

15.6.2. Затраты

Защита ИТ-инфраструктуры требует привлечения персонала, а следовательно, и денег для принятия, поддержки и проверки мер безопасности. Однако неспособность защитить ИТ-инфраструктуру также стоит денег (стоимость непроизведенной продукции; стоимость замены; ущерб для данных, программного или аппаратного обеспечения; потеря репутации; штрафы или компенсации в связи с невозможностью выполнения договорных обязательств). Как всегда, необходимо соблюдение баланса.

Приложение А

Фирма «Quick Couriers» («Быстрые курьеры»)

В данном примере рассматривается развитие молодой фирмы, столкнувшейся со всеми актуальными проблемами сервис-менеджмента. В конце каждого раздела ставятся вопросы, которые могут дать читателям пищу для размышлений.

Транспорт в Амстердаме в настоящее время так перегружен, что предоставление курьерских услуг с помощью автофургонов стало затруднительным. Поэтому после окончания учебы трое друзей Джейн, Джон и Питер решили заняться курьерскими услугами на велосипедах и открыли фирму Quick Couriers (QC). Фирма QC доставляет посылки в центр города, используя для этого велосипеды.

Сначала основатели фирмы Quick Couriers просто работали на себя, но потом они заключили договоры с международными курьерскими компаниями на получение и доставку посылок в центр города, из-за чего они уже не могли выполнять всю работу сами. Поэтому сейчас они используют студентов, работающих на них неполный рабочий день и развозящих посылки на велосипедах фирмы.

Джейн является ответственной за бухгалтерию, выписывание счетов, обработку заказов и поддержку деловых связей. Фирма Quick Couriers закупила программные приложения для бухгалтерии и Процесса Управления Взаимоотношениями.

Джон отвечает на телефонные звонки, рассматривает запросы заказчиков, занимается планированием и материально-техническим снабжением курьерской службы, а также передает сообщения курьеров Джейн и Питеру.

Питер отвечает за обслуживание велосипедов, заказывает детали и инструменты, планирует материально-техническое обеспечение и инструктирует курьеров.

Недавно три друга произвели анализ положения своей фирмы и определили свою концепцию и внутренние правила работы (policy). Концепция заключается в следующем: «Фирма Quick Couriers должна стать синонимом быстрой доставки в центре Амстердама и окружающих районах». Для реализации этого фирма начала рекламную кампанию и увеличила наем курьеров. Было запланировано оснащение курьеров пейджерами или мобильными телефонами. Был также сделан запрос о цене Интернет-системы, которой могли бы пользоваться заказчики для подачи заявок на курьеров и отслеживания доставки своих посылок. Другим рассматриваемым вариантом было расширение бизнес-операций путем открытия еще одного офиса в Гааге или Роттердаме. Кроме того, друзья решили, что для будущего компании критическое значение имеет постановка их бизнеса на более профессиональную основу. Поэтому они определили области, требующие особого внимания.

А.1. Управление Конфигурациями

Питер ведет журнальную регистрацию инструментов, инструкций по обслуживанию, велосипедов, трейлеров, деталей, непромокаемых накидок и шлемов для курьеров. Когда он болен или в праздники обслуживанием занимается его двоюродный брат Пол.

В настоящее время фирма имеет двадцать средств доставки (велосипедов и трейлеров), шестнадцать из которых постоянно используются. Остальные четыре или проходят техобслуживание, или могут использоваться как резерв. Фирма Quick Couriers использует технику двух моделей от разных поставщиков.

Для ускорения ремонта Питер собрал несколько подблоков/узлов наиболее дорогих и уязвимых компонентов. Например, у него есть комплекты дисковых тормозов, зубчатых передач, передние и задние колеса и осветительная арматура. Когда у него есть время, он чинит комплекты, заменяя изношенные или сломанные детали, но иногда для этой работы он пользуется услугами своей соседки Мэри, энтузиастки велосипедного движения, которая рано вышла на пенсию.

В мастерской у Питера имеются ящики с запасными деталями, кроме того, у него есть папка документов для отслеживания невыполненных заказов, отправленных поставщикам. Некоторые детали взаимозаменяемы с деталями обычных современных гоночных велосипедов.

Велосипедный гараж находится рядом с мастерской. Многие курьеры заходят, чтобы узнать новый график или починить свои велосипеды.

Из-за возросшего объема работы Питер не может больше вести бумажную документацию, и у него уходит слишком много времени на составление отчетов. Джейн жалуется по поводу всех счетов за детали и инструменты и интересуется, нельзя ли соблюдать экономию.

Сейчас Питер установил базу данных для ведения учета инвентаря, которую он назвал ConFig. Он держит в мастерской распечатку с описью деталей. Он также купил мощный гравер для маркировки внесенных в перечень деталей.

Вопросы:

1. Что послужило причиной для разработки этого процесса?
2. Кто вовлечен в процесс, кроме самого Питера?
3. Сделайте набросок сферы действия (scope) и степени детализации (level of detail) базы данных. Какие атрибуты конфигурационных единиц (CI) имеют значение для Питера?
4. Что используется для мониторинга состояния? Для чего нужно хранить историю состояний (status history)?
5. Приведите примеры некоторых вопросов, например, о тенденциях, на которые Питер может ответить сейчас с помощью базы данных, но не мог бы сделать раньше.
6. Как будет Питер заполнять базу данных?
7. Как может Питер обеспечить актуальное состояние базы данных?
8. Какие отчеты Питер будет предоставлять Джейн?

A.2. Управление Инцидентами и Служба Service Desk

При шестнадцати курьерах, постоянно находящихся в пути, нагрузка Джона по ответам на телефонные звонки все более возрастает. Он непрерывно получает заявки от заказчиков, жалобы о поздней доставке и сообщения от курьеров, чьи велосипеды сломались, или которые не могут доставить посылку из-за того, что адрес неправильный.

Джону все труднее уследить за всем, и он забывает делать важные звонки. Джейн также замечает, что про некоторые заказы забывают. Бумажки с записями теряются, и не понятно, кто над чем работает. Хотя делается все возможное для хорошего обслуживания заказчиков, невозможно определить, насколько быстро решаются проблемы. Заказчики начали жаловаться на недостатки обслуживания, и у всех на фирме создалось впечатление, что число заказов уменьшается.

В то же время Питер столкнулся с тем, что все большее маршрутов и посылок следует включать в план. Он создал базу данных — RoutePlan — для посылок и маршрутов, рассортировав их по почтовым индексам. Каждая поездка курьера охватывает несколько индексов при их оптимальной последовательности. Несколько курьеров могут обслуживать один и тот же маршрут.

Джона попросили отвечать на некоторые телефонные звонки самостоятельно. Например, он информирует заказчиков о диапазоне услуг, предоставляемых фирмой Quick Couriers, и регистрирует жалобы. Он также разбирается с тем, что случилось с посылками, и обязательно делает ответные звонки заказчикам. Теперь он имеет доступ к базе данных RoutePlan на компьютере Питера благодаря недавно установленному сетевому каналу между их компьютерами.

Для отслеживания всех сообщений и телефонных звонков Джон создал новую базу данных, TelLog. Джон использует TelLog для регистрации всех телефонных звонков и для назначения им категорий и кодов приоритета.

Вопросы:

1. Что вызвало развитие Службы Service Desk?
2. Какой тип Службы Service Desk первоначально использовался для данного процесса?
3. Какая информация об инциденте существенна при обработке обращения (звонка)?
4. Приведите примеры категорий и приоритетов.
5. Кому может позвонить Джон, если он не в состоянии решить проблему?
6. Эффективная связь с ремонтной мастерской имеет существенное значение. Какой термин используется для этого в библиотеке ITIL?
7. Как может фирма Quick Couriers убедиться в том, что обращения по инцидентам не пропущены, и кто отвечает за это?
8. Оказывается ли в данном случае поддержка бизнес-операциям (Business Operations support)? Если да, объясните как.
9. Какие информационные каналы к другим системам хотели бы вы создать, и с какой целью?
10. Какой отчет должен Джон представлять Питеру и Джейн?

А.3. Управление Проблемами

Благодаря базам RoutePlan для разработки маршрутов, TelLog для регистрации звонков и ConFig для регистрации инвентаря улучшился сервис и уменьшилась рабочая нагрузка. Фирма Quick Couriers теперь имеет тридцать курьеров на маршрутах, а Джон и Джейн поженились, и свадебной машиной», конечно же, был велосипед-тандем.

Джон теперь использует базу RoutePlan для планирования маршрутов. Привлекаемый к работе студент отвечает на телефонные звонки и может решить большую часть инцидентов с помощью предоставляемой Джоном документации. При возникновении новой проблемы, студент обращается за помощью к Питеру, Джону или Джейн, и затем документирует решение так, чтобы его можно было легко отыскать в следующий раз. Если курьер задерживается в пути из-за проблемы с велосипедом, студент из службе Service Desk отправляет запасную деталь на этот маршрут со следующим курьером. Если курьер не может справиться с проблемой, Питер доставляет ему другой велосипед на плейлере.

Однако Питера все еще беспокоит количество ремонтов дорожных велосипедов. Гонимые велосипеды легко ломаются, и они находятся в постоянном использовании. Все в значительной степени зависит от того, как курьеры преодолевают бордюры и выбоины. У фирмы Quick Couriers возникает впечатление, что велосипеды марки А меньше подвержены износу, чем велосипеды марки В, но в этом нет уверенности. Некоторые узлы выходят из строя более часто, чем другие, но непонятно, виновато ли в этом использование, сборка или модель.

Причиной беспокойства Джейн является количество потерянных посылок. Хотя они в конце концов обнаруживаются, она думает сделать работу курьеров более надежной. Курьеры получают премии за производительность, существует также приз за максимальное среднее число доставок в час. Но Джейн все же хочет получать больше информации об эффективности их работы и обслуживании заказчиков, чтобы при необходимости проводить инструктаж.

Джона попросили более глубоко проанализировать данные в базах TelLog, RoutePlan и ConFig для определения скрытых причин недостатков. Он предполагает, что ему придется объединить большое число архивных данных и провести анализ тенденций изменения.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Какие действия предпринимает Джон и с каким результатом?
4. Какую информацию хочет получить Джон от других систем?

5. Приведите примеры проблем и известных ошибок.
6. Каковы действия Джона в отношении известных ошибок?
7. Какие выводы Питер предоставляет Джейн и Джону?

A.4. Управление Изменениями

Изучая скрытые причины недостатков в работе курьеров, Джон узнал много полезного. Например, он обнаружил, что дисковые тормоза одной марки изнашиваются быстрее, чем другой, что некоторые курьеры более часто повреждают велосипеды по сравнению со своими коллегами, и что некоторые посылки теряются потому, что их кладут не в те курьерские трейлеры.

Джон дал некоторые рекомендации по этим проблемам. Так как эти рекомендации касались областей, которыми занимались Джейн и Питер, он обсудил с ними потенциальное действие предложенных мер и объем необходимой работы по их реализации. События прошедшей недели обсуждаются на еженедельных собраниях в понедельник утром. Поскольку предполагается, что Джон будет давать предложения по улучшениям работы регулярно, то теперь у него есть своя повестка дня и перечень предлагаемых действий.

Питера попросили испытать новый тип тормозов. После этого он собирается составить график обслуживания, на основе которого будет проводиться поэтапная замена тормозов. Работа по замене тормозов будет идти одновременно с плановым обслуживанием для того, чтобы велосипеды не выводились из эксплуатации слишком надолго или слишком часто.

Будут опробованы предложения по структурированному подходу к сортировке и распределению посылок, а также проведены собрания с курьерами, чьи велосипеды слишком часто ломаются.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Какие действия предпринимаются после того, как Джон представил свои предложения?
4. Опишите, как бы вы тестировали различные предложения, в том числе требуется ли план возврата к начальному состоянию. Что могло бы быть включено в план тестирования?
5. Что учитывается в планирование модификаций? Определите слабые места, риски, необходимые ресурсы и ожидаемое воздействие.
6. Что необходимо для закрытия незавершенных мероприятий? Какой другой процесс может быть использован?

A.5 Управление Релизами

Когда курьеры доставляют посылки заказчикам, они оставляют велосипеды на улице. Джон купил несколько надежных замков для предотвращения краж велосипедов. Велосипеды оснащены также отдельными замками на колесах и замками для трейлеров.

Запасные ключи Питер держит в коробке в ящике стола. Курьеры иногда теряют свои ключи, и приходится тратить много сил на поиски подходящего запасного ключа. По прошествии некоторого времени становится трудно определить, для каких замков потеряны также и запасные ключи. Фирме Quick Couriers приходится регулярно покупать новые замки, и сейчас, когда парк велосипедов расширяется, это обходится весьма дорого. Поэтому Питер решил улучшить введение ключами и их копиями.

Комплекты ключей определены для каждого велосипеда. Замки пронумерованы, и номера занесены в базу данных ConFig. Питер покупает шкаф для хранения ключей и их дубликатов.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Какие действия необходимо предпринять перед тем, как использовать новый комплект ключей?
4. Какие действия предпринимаются перед тем, как курьер может получить новый комплект копий ключей?
5. Заменяли бы вы весь комплект при выходе из строя одного замка? Как бы вы это назвали?
6. Какие действия вы бы предприняли при замене только одного замка? Как бы вы это назвали?

А.6. Управление Доступностью

Работы у фирма Quick Couriers становится все больше. При выходе велосипеда из строя на его ремонт уходит слишком много времени, окончания которого курьер с доставляемой посылкой должен ждать на обочине дороги. Кроме того, если курьер заболел, нарушается весь график доставки. Заказчики начинают жаловаться на слишком долгую доставку.

Джейн хочет сама заняться этим вопросом и включить его в планы компании. Данный вопрос охватывает обслуживание, время доставки и персонал. Целью компании является обеспечение всех возможностей для наиболее быстрой доставки. Среди возможных решений этого вопроса — организация мобильной ремонтной бригады, покупка телефонного коммутатора с системой меню, создание системы обработки и отслеживания заказов в Интернете. Все это требует значительных инвестиций.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Перечислите некоторые положительные моменты, угрозы и уязвимые места.
4. Используйте эту информацию для определения рисков.
5. Какие превентивные меры вы можете предложить?
6. Перечислите, что должно быть включено в план в части обслуживания, поставщиков и персонала.

А.7. Управление Мощностями

Рынок быстро меняется, фирма Quick Couriers получает новых заказчиков в других районах, рассматривается возможность распространения услуг на Гаагу и Роттердам, являющиеся густо населенными городами страны. Питер также обдумывает открытие нового офиса в международном аэропорту Шипхол.

У Джейн есть информация о необходимом уровне кадрового обеспечения для каждого маршрута, полученная из практического опыта. Она использовала систему RoutePlan для создания отчета, показывающего по каждому маршруту сколько посылок доставляются в каждый день недели, в какое время дня маршруты наиболее загружены, и сколько посылок входят в трейлер. Она использовала средние значения в качестве базового уровня и определила процентное отношение выше и ниже базового уровня для каждого месяца и времени дня. Она хочет использовать эту информацию для планирования оборудования и персонала.

Джейн использует эту информацию для подготовки отчета об ожидаемом расширении и необходимых затратах и капиталовложениях.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Приведите примеры деятельности по моделированию.
4. Как можно справиться с пиковыми нагрузками без развертывания дополнительных мощностей?
5. Какие действия помогают в расчете ресурсов при открытии нового маршрута?
6. Что должно включаться в план возможностей?

A.8. Управление Непрерывностью ИТ-сервиса

На прошлой неделе сгорело здание по соседству с фирмой Quick Couriers. Это по-настоящему испугало Джейн, Джона и Питера. Их нынешнее помещение очень удобно, а поиск нового офиса в Амстердаме весьма труден. Они осознали, что если бы сгорело их здание, месяцы ушли бы на то, чтобы снова вернуться в бизнес.

Поэтому они решили включить опции восстановления в случае чрезвычайных обстоятельств в свои планы по поиску нового офиса в южной части Амстердама. Они также собираются рассмотреть альтернативные варианты поблизости от нынешнего местоположения, которые могли бы использоваться как временная база для обслуживания маршрутов в центре города. Их план включает следующие позиции:

- размещение;
- средства доступа;
- персонал;
- электронные файлы и компьютерные системы;
- оборудование;
- посылки заказчиков.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Какие причины заставляют компанию составлять план на случай чрезвычайных обстоятельств?
4. Каковы угрозы, активы компании и точки уязвимости?
5. Используйте эту информацию для определения рисков.
6. Какие превентивные меры могут быть приняты и при каких рисках необходимы удаленные помещения для восстановления на случай чрезвычайных обстоятельств?
7. Каким термином библиотеки ITIL обозначается план на случай чрезвычайных обстоятельств, предлагающий использование ИТ-средств другой организации?
8. Определите позиции, которые должны быть включены в план перемещения на другое местоположение, и опишите способы тестирования такого плана.
9. Какова зависимость плана обеспечения непрерывности ИТ-сервиса от плана возможностей и плана повышения доступности (например, новый офис)?
10. Каково влияние процесса Управления Изменениями (Консультативного комитета по изменениям — CAB)? Приведите пример для данного случая.

А.9. Управление Финансами

Диапазон услуг, предоставляемых фирмой Quick Couriers, расширяется. Фирма использует сниженные тарифы для доставки в непиковые периоды времени, наценки за срочную доставку и едки за большие объемы. Заказчики могут использовать Интернет для подачи заявок и для отслеживания местонахождения своих посылок. Однако некоторые из работников Quick Couriers уволились и основали собственное дело, что повлияло на качество и стоимость услуг.

Возросли также затраты, связанные с поддержкой услуг. Фирма становится все более зависимой от эффективных ИТ-средств. Джейн заключила договор с поставщиком услуг сети Интернет на предоставление выделенной линии, и фирма Quick Couriers приняла на работу сетевого администратора, чтобы обеспечить поддержку работы системы. Есть ремонтная бригада, постоянно годящаяся в разъездах. Административные расходы увеличились из-за роста численности персонала. Вложены средства в помещения, так что теперь амортизационные отчисления стали существенным фактором в бухгалтерии. Экспресс-услуги по работе курьеров должны быть доступны в любое время, а это означает, что иногда курьеры простаивают.

Становится все труднее установить цены, которые бы покрывали затраты. Джейн хочет поддерживать некоторые услуги (которые их конкуренты также оказывают) путем назначения низких цен, но должна соблюдать осторожность, чтобы новые цены не привели к убыткам от основной деятельности.

Джейн хочет ввести централизованную систему учета расходов для получения информации о расходах, связанных с предоставлением каждой услуги. Она надеется, что сможет компенсировать потери на некоторых услугах за счет прибыли от других услуг, если будет получать больше информации о расходах на каждую услугу.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Приведите примеры постоянных и переменных затрат, а также прямых и косвенных затрат.
4. Приведите пример каталога услуг и средств производства, необходимых для различных услуг.
5. Составьте суммарный план цен.

А. 10. Управление Уровнем Услуг

Джейн хочет привязать к своей фирме постоянных клиентов. Поэтому она стремится поддерживать с ними более тесные контакты и заключать долгосрочные договоры на обслуживание. Вместо того, чтобы платить за каждую посылку или услугу, постоянные заказчики могли бы платить фиксированную ежемесячную плату. Это обеспечит фирму постоянным доходом, что, в свою очередь, облегчит планирование услуг.

Из-за того, что большое число велосипедов постоянно находятся на линии, фирма Quick Couriers становится все более зависимой от поставщиков деталей и других услуг. Поэтому Джейн хочет заключить с ними договоры, гарантирующие точное время поставки.

Фирма Quick Couriers приняла на работу нового сотрудника на должность представителя по работе с крупными клиентами (account manager). Его задачей является преобразование потребностей заказчиков в планы разработки новых или модифицированных услуг. После заключения внешних договоров он может начать подготовку нового каталога.

Вопросы:

1. Что вызвало разработку этого процесса?
2. Кто вовлечен в процесс и в какой роли?
3. Опишите функции представителя по работе с крупными клиентами.
4. Приведите пример рамочного соглашения с постоянным заказчиком.
5. Как гарантируются услуги, согласованные с заказчиком?
6. Что может включаться в План обеспечения качества сервиса (SQP) компании?
7. Если бы вы были заведующим представителем по работе с крупными клиентами, с кем бы вы заключили OLA?
8. Кому бы вы докладывали о достижениях в предоставлении услуг?

Приложение В 1. Акронимы

ACU	Accommodation Cost Unit.....	Статья учета затрат на размещение
AMDB	Availability Management Database.....	База данных управления доступностью
BCM.....	Business Continuity Management.....	Управление непрерывностью бизнеса
BSC.....	Balanced Score Cards.....	Карты сбалансированных балльных оценок
CA.....	Cost Accounting.....	Учет затрат
CAB.....	Change Advisory Board.....	Консультативный комитет по изменениям
CAB/EC	Change Advisory Board/.....	Консультативный комитет по изменениям /
	Emergency Committee.....	Комитет по срочным изменениям
CCTA	Central Computer and.....	Центральное агентство по вычислительной
	Telecommunications Agency.....	технике и телекоммуникациям (Великобритания)
CDB	Capacity Database.....	База данных мощностей
CFIA.....	Component Failure Impact Analysis ...	Анализ степени воздействия сбоя компонентов
CI.....	Configuration Item.....	Конфигурационная единица
CMDB	Configuration Management Database..	Конфигурационная база данных
CMM	Capability Maturity Model.....	Модель зрелости (CMM)
CRAMM	CCTA Risk Analysis.....	Метод анализа и управления рисками CCTA
	and Management Method.....	
CRM.....	Customer Relationship Management...	Управление взаимоотношениями с заказчиками
CSF.....	Critical Success Factor.....	Критический фактор успеха
CTI	Computer Telephony Integration.....	Компьютерно-телефонная интеграция
DHS	Definitive Hardware Store.....	Склад эталонного аппаратного обеспечения
DoS	Denial of Service.....	Отказ в обслуживании
DSL.....	Definitive Software Library.....	Библиотека эталонного программного
		обеспечения (Фонд алгоритмов и программ)
ECU	Equipment Cost Unit.....	Затраты на оборудование
EFQM.....	European Foundation for Quality.....	Европейский фонд управления качеством
	Management.	
EXIN.....	Examination INstitute.....	Экзаменационный институт EXIN
FSC.....	Forward Schedule of Change.....	Согласованный план изменений
FTA.....	Fault Tree Analysis.....	Анализ дерева неисправностей
HRM.....	Human Resource Management.....	Управление персоналом
ICT	Information and Communication.....	Информационные и телекоммуникационные

	Technology	технологии
ISEB	Information Systems Examination Board	Экзаменационный институт ISEB
ISO	International Standards Organisation...	Международная организация по стандартизации
IT.....	Information Technology	Информационные технологии
ITIL.....	Information Technology Infrastructure Library	Библиотека передового опыта организации ИТ
ITSCM	IT Service Continuity Management	Управление непрерывностью ИТ-сервисов (услуг)
ITSM.....	IT Service Management	ИТ Сервис-менеджмент
ITSMF	IT Service Management Forum	Форум по ИТ Сервис-менеджменту
IVR.....	Interactive Voice Response	Интерактивное речевое меню
KPI	Key Performance Indicator	Ключевой показатель эффективности
LAN.....	Local Area Network	Локальная вычислительная сеть LAN
MTBF	Mean Time Between Failures	Среднее время между сбоями
MTBSI	Mean Time Between System Incidents	Среднее время между системными инцидентами
MTTR	Mean Time To Repair	Среднее время ремонта
OCU	Organization Cost Unit	Организационные затраты
OGC	Office of Government Commerce	Государственная торговая палата (Великобритании)
OLA.....	Operational Level Agreement	Соглашение об оперативном уровне услуг
PC	Personal Computer	Персональный компьютер
PI.....	Performance Indicator	Показатель качества
PIR	Post-Implementation Review	Анализ результатов внедрения
RFC.....	Request For Change	Запрос на изменение
SCU.....	Software Cost Unit	Затраты на программное обеспечение
SIP.....	Service Improvement Program	Программа улучшения сервиса (услуг)
SLA.....	Service Level Agreement	Соглашение об уровне услуг
SLM.....	Service Level Management	Управление уровнем услуг
SLR.....	Service Level Requirements	Требования по уровню услуг
SMART	Specific, Measurable, Appropriate, Realistic and Time-bound	Конкретный (Specific), измеримый (Measurable), уместный и соответствующий ситуации (Appropriate), реалистичный (Realistic) и определенный по времени (Time-bound)
SOA.....	System Outage Analysis	Анализ сбоев системы
SPOF	Single Point Of Failure	Критическая точка сбоя
SQP.....	Service Quality Plan	План обеспечения качества услуг (сервиса)
TCU	Transfer Cost Unit	Трансфертные затраты
TOP.....	Technical Observation Post	Пункт технического наблюдения
UC.....	Underpinning Contract	Внешний договор
UPS.....	Uninterruptible Power Supply	Источник бесперебойного питания
VOIP.....	Voice Over Internet Protocol	Речевая связь через Интернет по протоколу VoIP
WAN	Wide Area Network	Глобальная сеть WAN

В.2. Дополнительный материал

ПРЕДМЕТ	НАЗВАНИЕ	ИЗДАТЕЛЬ	ISBN
Service Support	Service Support	OGC/HMSO	0 11330015 8
Service Delivery	Service Delivery	OGC/HMSO	0 11330017 4
Service Management	Security Management	OGC/HMSO	011 330014 X
Applications	Application Management	OGC/HMSO	0 11330866 3
Infrastructure	ICT Infrastructure Management	OGC/HMSO	0 11330865 5
Implementation	Planning to Implement Service Management	OGC/HMSO	011 330905 8
General ITSM	The Guide to IT Service Management	Addison Wesley	0 20 173792 2
Humor	Not The IT Infrastructure Library	Giggle Production	0 95 334690 0

В.3. Веб-сайты

OGC.....<http://www.ogc.gov.uk>
ITIL.....<http://www.itil.co.uk>
EXIN.....<http://www.exin.nl>
ISEB.....<http://www.bcs.org.uk/iseb>
itSMF-AU.....<http://www.itsmf.org.au>
itSMF-BE.....<http://www.itsmf.be>
itSMF-CA.....<http://www.itsmf.ca>
itSMF-DE.....<http://www.itsmf.de>
itSMF-NL.....<http://www.itsmf.nl>
itSMF-SA.....<http://www.itsmf.org.za>
itSMF-UK.....<http://www.itsmf.com>
itSMF-USA.....<http://www.itsmf.net>
ITSM PORTAL.....<http://en.itsmportal.net>
ITIL/ITSM World.....<http://www.itil-itsm-world.com>
The ITIL Tooling Page.....<http://tools.itsmportal.net>
ITIL world.....<http://www.itilworld.com>
Loyalist College.....<http://www.itilexams.com>