Комплекс мер по обеспечению непрерывности функционирования и доступности ИС

Подход к разработке

Максим Гусляев, ведущий консультант
17/11/2011

Содержание

1. Требования бизнеса к ИТ-сервисам
2. Как связать бизнес и ИТ?
3. Описание состава и последовательности выполнения работ
4. Анализ воздействия простоев на бизнес (BIA)
5. Анализ технологических рисков
6. Обзор организационных и технических мер защиты

ИТ в контексте интересов бизнеса

Оптимизация расходов на инженерную инфраструктуру ЦОД, ИТ-инфраструктуру (серверы, системы хранения, сети) а также эксплуатацию ИТ, что предусматривает повышение эффективности данных компонентов

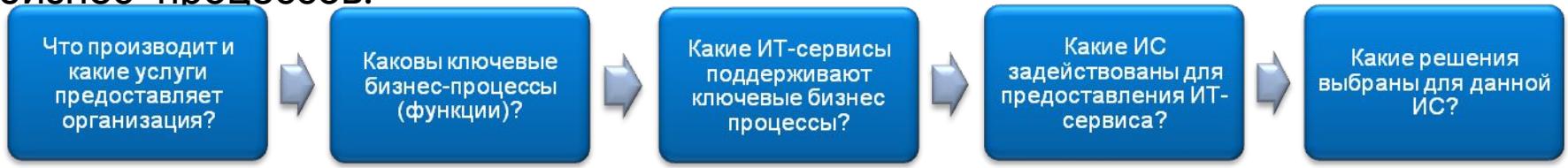
Снижение рисков через повышение доступности ИТ сервисов, соблюдение SLA, а также упрощение инфраструктуры для минимизации влияния человеческого фактора

Адаптация к изменениям через возможность масштабирования ИТ для запуска новых направлений деятельности организации, обеспечения роста бизнеса и повышения гибкости ИТ при реагировании на меняющиеся запросы

Связываем бизнес и ИТ

При разработке и/или трансформации ИС и ИТ-инфраструктуры необходимо учитывать планы по развитию бизнеса, а также требования и характеристики ключевых поддерживаемых ими бизнес-процессов с тем, чтобы:

- Не допустить неоправданно высоких затрат на отказоустойчивые решения, которые, может быть, и не нужны;
- Реализовать решения, направленные на снижение действительно существенных
рисков в отношении непрерывности существующих или проектируемых бизнес-процессов.



Состав и последовательность выполнения работ

Анализ влияния простев на бизнес
(Business Impact Analysis – BIA)

Цель

- Выявить прямое и косвенное влияние на бизнес в результате утраты критически важных бизнес-процессов и функций
- Разработать согласованные с бизнес-требованиями цели по восстановлению работоспособности бизнес-процессов и ИТ-сервисов после сбоя.

Результат

- Разработка категорий восстановления, отнесение бизнес-процессов к соответствующим категориям;
- Определение и документирование RTO и RPO для каждой бизнес-функции/процесса;
- Выяснение взаимосвязей между наиболее критичными бизнес-функциями;
- Установление соответствий между бизнес-процессами, ИТ-сервисами, ИС и элементами ИТ инфраструктуры.

Терминология

Ключевой бизнес-процесс (бизнес-функция)

- Процесс, жизненно необходимый для функционирования компании. Простой ключевого бизнес процесса ведет к недопустимым для компании последствиям (причем негативный эффект может быть отложенным).

Допустимый диапазон потери данных

Recovery Point Objective, RPO

- Отрезок времени, предшествующий срыву бизнес-процесса, за который допускается невосполнимая потеря введенных данных, результатов работы и пр. Данный параметр является одним из важнейших результатов формализованного анализа влияния простоев ИТ систем на бизнес-процессы.

Целевое время восстановления

Recovery Time Objective, RTO

- Время, за которое должно быть восстановлено функционирование ключевого процесса и/или процесса, от которого он зависит. Причиной сбоя в данном контексте может являться кризисная ситуация, чрезвычайное происшествие или инцидент.

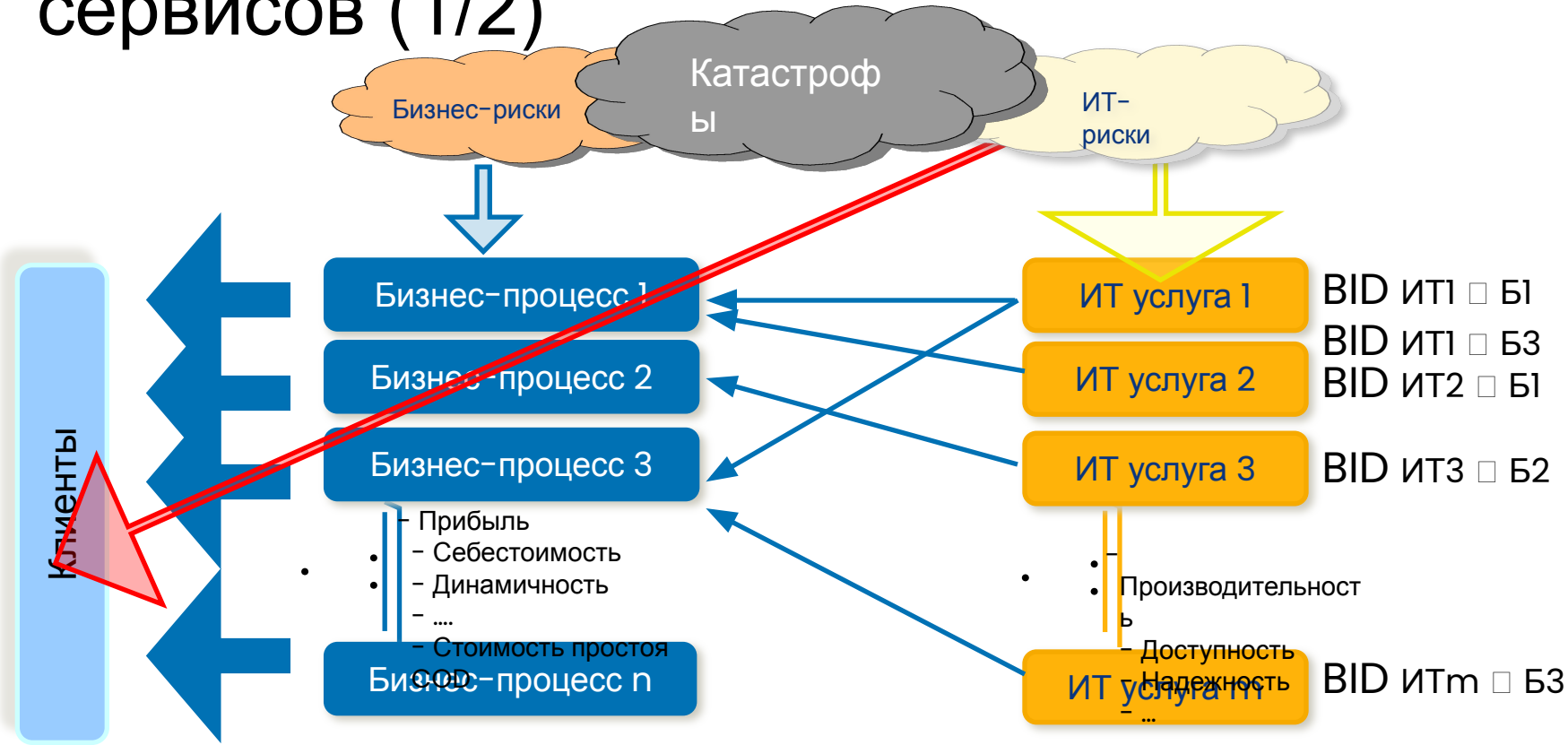
Анализ ключевых бизнес-процессов

Бизнес-процесс (функция)	Режим испл-я	Влияние отказа во времени								
		<30 мин	30 мин – 2 hrs	2 – 4 час	4 – 8 час	8 – 24 час	24 час – 3 дн	3 – 5 дн	5 – 10 дн	10 – 15 дн
Процесс № 1	24x7									
Процесс № 2	24x7									
Процесс № 3	24x7									
Процесс № 4	24x7									
Процесс № 5	8x5									
Процесс № 6	24x7									
Процесс № 7	8x5									
Процесс № 8	24x7									

Проводится анализ влияния простоев бизнес-процессов на Организацию, на базе чего в дальнейшем формулируются требования к времени восстановления (RTO) ИС, поддерживающих эти бизнес-процессы.

hp invent

Зависимость бизнес-процессов от ИТ-сервисов (1/2)

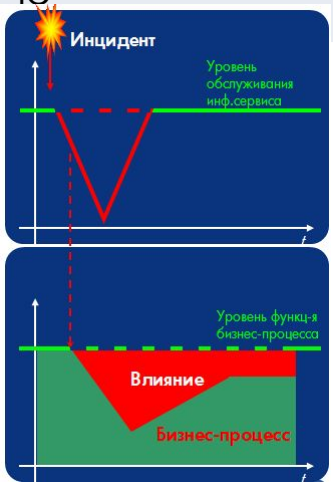


RTO ИТx = min (RTO ИТx □ Б1 ; RTO ИТx □ Б2 ;... RTO ИТx □ Бy)

Зависимость бизнес-процессов от ИТ-сервисов (2/2)

Информационная система/ сервис	Бизнес-процесс 1	Бизнес-процесс 2	Бизнес-процесс 3
Service Desk	x	x	x
CRM			x
…			
1С	x	x	

Определяется роль информационных систем и сервисов в функционировании бизнес-процессов.



- Какие бизнес-функции зависят от данного информационного сервиса?
- Как скоро после сбоя информационного сервиса бизнес ощутит негативное влияние?
- Есть ли обходные пути, позволяющие работать при недоступном информационном сервисе?
- Как нагнать отставание?
- Каковы затраты на преодоление отставания?
- Можно ли вообще компенсировать потерянное время?

Классификация ИС по степени критичности

Информационная система/ сервис	Класс критичности	RTO	RPO
Service Desk	1 (Mission Critical)	4 часа	X
CRM		4 часа	X
…	1 (Mission Critical)		
1C	2 (Business Critical)	8 часов	Y

Приоритеты восстановления ИС

Класс 1
Mission Critical
Приоритет:
неотложный

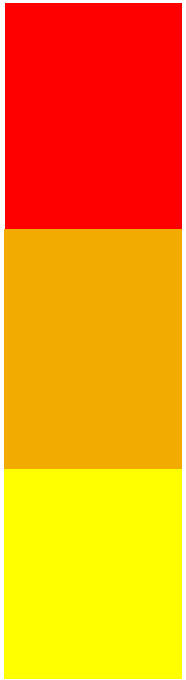
- Длительность восстановления – менее 4 часов.
- Процесс жизненно и стратегически важен для работы компании.
- Существенное нарушение ключевых бизнес-процессов.
- Заметное негативное влияние сбоя проявляется немедленно и продолжает сказываться даже после быстрого устранения сбоя.
- Серьезные ограничения и правовая ответственность.

Класс 2
Business Critical
Приоритет:
критичный

- Длительность восстановления – от 4 часов до 8 часов.
- Процесс необходим для ежедневной работы компании.
- Сбой одновременно затрагивает как внешних клиентов, так и несколько департаментов компании.
- Заметное негативное влияние сбоя проявляется немедленно.

Класс 3
Business Oper.
Приоритет:
важный

- Длительность восстановления – от 8 до 24 часов.
- Процесс необходим для поддержания внутренней оперативной деятельности.
- Долговременный сбой окажет заметный негативный эффект.



Требования к архитектуре ИС (1/2)

Для каждого класса критичности разрабатывается набор требований, в совокупности определяющих целевое состояние, позволяющее уложиться в значения RTO/RPO:

- Методы защиты приложения
- Методы защиты данных в оперативном доступе
- Методы резервного копирования данных
- Дублирование персонала
- Процессы эксплуатации
- Мониторинг
- Инфраструктура ЦОД
- Уровень внешней технической поддержки

Требования к архитектуре ИС (2/2)

Класс	Методы защиты приложения	Методы защиты данных в оперативном доступе	Методы резервного копирования	Дублирование персонала	Процессы эксплуатации	Мониторинг	Инфраструктура ЦОД	Внешняя техническая поддержка
МС	Failover кластер (hot-standby) Load-balancing Серверы high-end или Mid-range Виртуализация	Репликация данных (dual storage) Oracle RAC Business copy or snapshots на базе дисковых массивов High-end СХД SAN Репликация Archlogs	Enterprise back-up solution ZDT back-up	Дежурная смена 24x7 Дублирование специалистов	План и процедуры аварийного восстановления Учения Change и configuration management Регламентные окна для обслуживания	Упреждающий мониторинг	Резервный ЦОД, способный выдержать полную нагрузку	MCP и CS 6h CTR + proactive maintenance
ВС	Warm-standby или Dedicated cold-standby	High-end или mid-range СХД SAN Репликация Восстановление из резервных копий	Enterprise back-up solution	Дежурная смена 24x7 Дублирование специалистов	План и процедуры аварийного восстановления Регламентные окна	Мониторинг сбоев	Резервный ЦОД	CS и P24 proactive maintenance
ВО	Dedicated cold-standby	Восстановление из резервных копий SAN, NAS, DAS	Enterprise back-up or local solution	Дублирование специалистов	План и процедуры аварийного восстановления	Мониторинг сбоев	Контракты на поставку, резервные комплектующие на складе	P24 и NBD Fix hours CTR
ОР	Не формализованы	Не формализованы	Не формализованы	Не формализованы	Не формализованы	Не формализованы	Не формализованы	Не формализованы

hp invent

Анализ текущей архитектуры ИС, процессов и практик управления ИТ

Приложение/система	Класс	Методы защиты приложения	Методы защиты данных в оперативном доступе	Методы резервного копирования	Дублирование персонала	Процессы эксплуатации	Мониторинг	Инфраструктура ЦОД	Внешняя техническая поддержка	Величина риска
ИС 1	МС	Осуществляется балансировка нагрузки между 4 серверами приложений (blade workstations в одном шасси). Используется 1 сервер БД (blade server в другом шасси).	Локальные жесткие диски серверов приложений и БД в RAID 1. Сервер БД использует StorageWorks SB40c для расширения дискового пространства.	Не осуществляется.	Да (1 сотрудник круглосуточной дежурной смены, а также 2 сотрудника технической поддержки, работающие по графику 8x5 - по вопросам СПО и инфраструктуры, а также 1 сотрудник дежурной смены Компании X и сотрудники Компании X, работающие по графику 8x5).	Планы аварийного восстановления отсутствуют, учения по восстановлению не проводятся. Окна регламентного обслуживания не назначены. Развернута тестовая среда, включающая 1 сервер приложений, 1 Management Server, 1 Report Server, 1 Technology Server. Разработана документация на систему, включающая описание технический решений.	Осуществляется средствами подсистемы мониторинга и управления данной ИС. Имеются 1 Management Server, 1 Report Server, 1 Technology Server (blade workstations в том же шасси, где установлены серверы приложений). Мониторинг событий ИБ не осуществляется.	Все компоненты системы размещены на одной площадке ЦОД Головного офиса. Серверы приложений на базе ProLiant xw460c Blade Workstation в шасси BLc7000. Сервер БД на базе BL680c G5 в другом шасси.	Техническая поддержка ППО осуществляется Компанией X. Поддержка СПО и аппаратного обеспечения есть.	2,13
ИС 2	МС	ПО "толстого" клиента BS-Client установлено на нескольких АРМ бухгалтерии и казначейства. Однако, отправка данных в банк осуществляется через 1 физический сервер отправки. В качестве сервера БД используется сервер Oracle ИС "Галактика".	Локальные жесткие диски серверов приложений и БД в RAID 1. Сервер БД подключен к Modular SAN Array 1000 с RAID 5.	Резервное копирование БД Oracle осуществляется 1 раз в сутки на основе экспорта и передачи экспортируемого двоичного файла на сервер резервного копирования (в порядке, установленном для Галактика).	Нет. Сопровождение осуществляет 1 сотрудник ДТТО.	Планы аварийного восстановления отсутствуют, учения по восстановлению не проводятся. Окна регламентного обслуживания не назначены.	Доступность сервера Omega отслеживается Alchemy Eye. Мониторинг событий ИБ не осуществляется.	Все компоненты системы размещены на одной площадке ЦОД Головного офиса. Сервер передачи данных Omega на базе HP Proliant DL360 G3.	Поддержка BSS не приобретена. Консультации оказываются специалистами Банка. Поддержка СПО и аппаратного обеспечения отсутствует.	2,19

hp invent

Обзор организационно-технических мер (1/3)

- Методы защиты приложения
  - Кластеризация аппаратных платформ, территориальное разнесение компонентов между основным и резервным ЦОД
    - VmWare Cluster, Hyper-V Cluster, Windows Server Failover Clustering и т.д.
    - HP Metrocluster, HP Contibentalcluster
  - Виртуализация и консолидация серверов и приложений
  - Холодный резерв
  - Модернизация и апгрейд серверов (увеличение объема ОЗУ, кол-ва процессоров, изоляция и перераспределение аппаратных ресурсов между приложениями – nPartitioning, vPartitioning, оптимизация СХД и т.д.)
  - Балансировка нагрузки
  - Реализация отказоустойчивой сетевой топологии, Teaming для сетевых интерфейсов серверов
  - Обнаружение уязвимостей в исходном коде и web приложениях и защита от сетевых атак
    - HP Fortify
    - HP Webinspect
    - HP Tippingpoint
- Методы защиты данных в оперативном доступе
  - Локальный RAID массив
  - Репликация данных
  - High-end СХД
  - SAN

hp invent

Обзор организационно-технических мер (2/3)

- Методы резервного копирования данных
  - Разработка и реализация архитектуры резервного копирования: централизованное решение vs локальное решение
    - HP Dataprotector
    - Резервное копирование средствами Ignite/UX
  - Разработка регламента резервного копирования
  - Организация хранения резервных копий за пределами основной площадки
  - Регулярное тестирование целостности резервных копий
- Дублирование персонала
  - Дежурная смена 24x7
  - Дублирование специалистов
- Процессы эксплуатации
  - Разработка планов аварийного восстановления
  - Проведение учений
  - Окна регламентного обслуживания оборудования
  - Внедрение процессов управления изменениями и конфигурациями
  - Мониторинг сбоев

Обзор организационно-технических мер (3/3)

- Мониторинг
  - Построение централизованной системы мониторинга состояния приложений и инцидентов
    - HP Operations Manager
    - HP System Insight Manager
    - HP ArcSight
- Инфраструктура ЦОД
  - Создание резервного ЦОД, способного выдержать полную или частичную нагрузку в случае выхода из строя основного
  - Создание резервного запаса комплектующих на складе
  - Термическое моделирование ЦОД, оптимизация циркуляции воздушных масс в серверном помещении и расположения телекоммуникационных шкафов для недопущения возникновения зон перегрева
- Уровень внешней технической поддержки
  - Mission Critical Partnership и Critical Service, 6 часов Call-to-Repair Hardware Support + proactive maintenance
  - Critical Service и Proactive 24 + proactive maintenance
  - Proactive 24 и NBD, fix-hours Call-to-Repair Hardware Support

Организационная структура проекта (сервиса)

Спасибо за внимание