6.1. Процесс: IT SERVICE CONTINUITY MANAGEMENT - Управление непрерывностью услуг

Управление непрерывностью услуг (IT Service Continuity Management или ITSCM) - процесс, ответственный за *управление рисками*, которые влияют на услуги. ITSCM обеспечивает возможность поставщику услуг постоянно предоставлять минимально согласованный Уровень услуг, через снижение рисков до приемлемого уровня и Планирование восстановления услуг.

Основная цель Управления непрерывностью услуг (далее просто Управление непрерывностью) - поддерживать *процесс Управления Н*епрерывностью Бизнеса.

Управление непрерывностью бизнеса (Business Continuity Management или BCM) - *бизнес-процесс*, отвечающий за *управление рисками*, которые могут серьезно повлиять на бизнес. *BCM* защищает интересы ключевых заинтересованных сторон, репутацию, бренд и *деятельность* по созданию ценности. Процесс *BCM* включает в себя снижение рисков до приемлемого уровня и планирование способов восстановления бизнес-процессов в случае нарушения бизнеса. *BCM* устанавливает цели, охват и требования по отношению к Управлению непрерывности ИТ-услуг.

В настоящее время технологии являются основным компонентом многих бизнес процессов, поэтому обеспечение их непрерывности и доступности является необходимым для существования бизнеса в целом. ITSCM управляет способностью услуг и их компонентов к восстановлению.

Промежуточные цели ITSCM:

1. Управление набором Планов обеспечения непрерывности услуг и Планов восстановления услуг, которые являются частью Планов обеспечения непрерывности бизнеса.

План обеспечения непрерывности услуг (IT Service Continuity Plan) - план, определяющий шаги, необходимые для восстановления одной или нескольких услуг. План также должен определять события, которые являются основанием для его инициации, людей, которые должны быть задействованы, средства коммуникаций и т.п.

План обеспечения непрерывности бизнеса (Business Continuity Plan или BCP) - план определяет шаги, необходимые для восстановления бизнес-процессов в случае нарушения их функционирования. План также должен содержать информацию о событиях, которые являются основанием для его инициирования; людях, которые должны быть задействованы в реализации плана; средствах коммуникаций и т.п.

2. Завершение Анализа влияния на бизнес в части гарантии управления планами обеспечения непрерывности в соответствии с изменяющимися требованиями и потребностями бизнеса;
3. Сопровождение Анализа рисков и менеджмента, в частности при взаимодействии с бизнесом и процессами Управления доступностью и Управления безопасностью, которые управляют услугами в соответствии с согласованным Уровнем услуг;

4. Предоставление рекомендаций и руководств другим областям IT в вопросах, связанных с непрерывностью и восстановлением услуг;
5. Обеспечение механизмов непрерывности и восстановления, которые позволят достигнуть целевых показателей, установленных бизнесом;
6. Оценка влияния изменений на Планы обеспечения непрерывности услуг и Планы восстановления услуг;
7. Проактивное улучшение непрерывности услуг там, где это экономически эффективно;
8. Ведение переговоров и заключение контрактов с поставщиками об обеспечении необходимой способности к восстановлению в целях поддержки непрерывности (с участием процесса Управления поставщиками).

Управление непрерывностью фокусируется на значимых негативных событиях, которые *ITIL* называет "катастрофами" для бизнеса.

Менее значимые события рассматриваются в рамках процесса Управления инцидентами. То, является ли какое-то конкретное событие катастрофой, зависит от организации, в которой оно произошло.

Размер и *значимость* негативного влияния события на бизнес, например, финансовые потери или потеря репутации, измеряется в рамках Анализа влияния на бизнес.

Анализ влияния на бизнес определяет минимальные требования к критичности, конкретные требования к технологиям и услугам определяются в рамках Управления непрерывностью.

ITSCM главным образом рассматривает *активы* IT и конфигурации, которые поддерживают *бизнес-процессы*. В случае катастрофы бизнесу необходимо перестроиться на альтернативную рабочую локацию. При этом необходимо предоставить такие элементы как удобство офиса для персонала, копии критических бумажных отчетов, услуги курьеров и телефонную *связь* для связи с клиентами и партнерами.

В этой связи Управление непрерывностью должно учитывать количество и месторасположение офисов организации, а также услуги, предоставляемые в каждом из них.

В рамках Управления непрерывностью должны выполняться следующие деятельности:

1. Согласование границ ITSCM и применяемых политик;
2. Анализ влияния на бизнес для количественной оценки влияния потери услуги на бизнес;
3. Анализ рисков - идентификация и оценка рисков с целью определения потенциальных угроз непрерывности и оценки вероятности их осуществления. Сюда также входит применение механизмов управления угрозами там, где это экономически эффективно;
4. Формирование стратегии ITSCM, интегрированной в стратегию *BCM*.
5. Формирование Планов обеспечения непрерывности, интегрированных в планы *BCM*.
6. Тестирование планов обеспечения непрерывности;
7. Непрерывное осуществление планов и управление ими.

Рис. 6.1. Жизненный цикл ITSCM

ITSCM циклически повторяется на всем жизненном цикле услуги и гарантирует то, что однажды разработанные планы по восстановлению и обеспечению непрерывности услуг будут соответствовать в дальнейшем приоритетам бизнеса и Планам обеспечения непрерывности бизнеса.

На рис. 6.1 также показана роль *BCM* в ITSCM.

Стадии инициализации и формирования требований относятся к *BCM*.
ITSCM должен только участвовать в этих стадиях, чтобы поддержать *BCM* и понять связи между бизнес-процессами и влияние потери услуг на них. В результате этих начальных стадий *BCM* формирует Стратегию обеспечения непрерывности бизнеса. Для ITSCM первой серьезной задачей становится сформировать свою стратегию, которая сделает возможной и поддержит Стратегию непрерывности бизнеса. Рассмотрим стадии жизненного *цикла* ITSCM.

Стадия 1 - *Запуск*

Эта стадия ITSCM состоит из следующих действий:

- Формирование политики обеспечения непрерывности - должно быть осуществлено как можно быстрее. Политика, как минимум, должна определять цели и моменты и вопросы, на которые менеджмент должен обратить внимание;
- Определение терминов охвата и компетенции - определение границ ITSCM и распределение ответственности для всего персонала в организации;
- Распределение ресурсов - формирование окружения для обеспечения непрерывности бизнеса, требующего значительных ресурсов как денежных, так и людских.
- Определение проекта для организации процесса ITSCM и структуры его контроля - ITSCM и *BCM* являются сложными процессами, требующими тщательной организации и контроля.
- Согласование проекта и планов качества - планы обеспечивают контроль проекта и его применимость для различных ситуаций.

Стадия 2 - Требования и стратегия

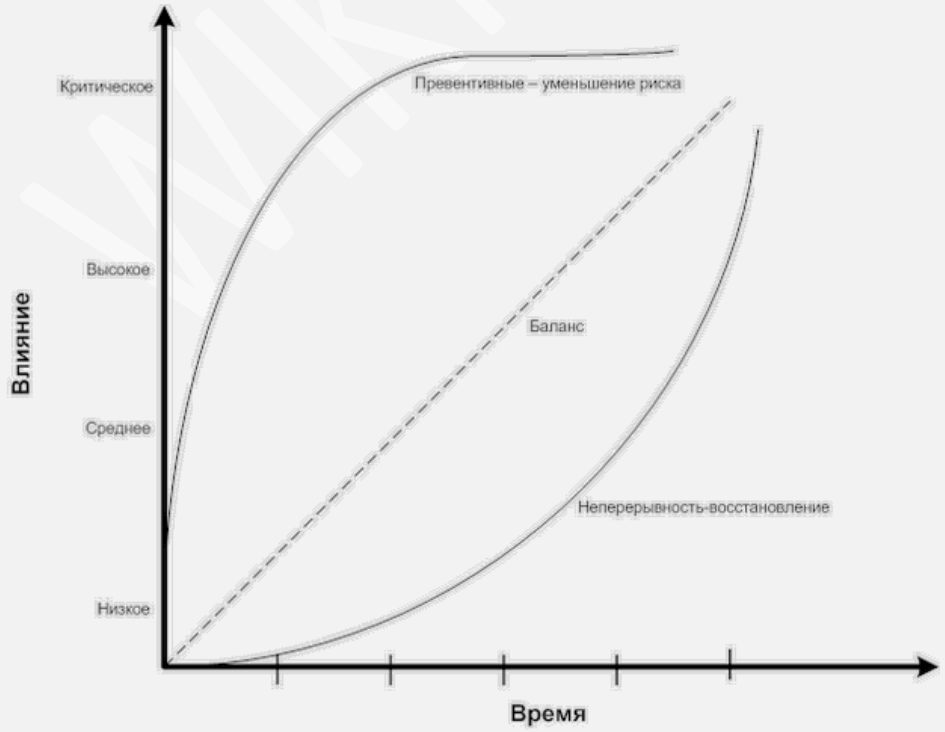
Установление требований бизнеса к непрерывности услуг является критически важным, так как именно от этого этапа зависит *устойчивость* организации к катастрофам и соответствующие *затраты*. Если требования некорректны или пропущена какая-то важная *информация*, все *механизмы* ITSCM будут неэффективны. Эта стадия разделяется на две под-стадии:

- Требования - Анализ влияния на бизнес и оценка рисков
- Стратегия - стратегия формулирует меры уменьшения риска и опции восстановления.

Анализ влияния на бизнес (Business Impact Analysis или BIA) - *деятельность* в рамках процесса Управления непрерывностью бизнеса, которая определяет критичные бизнес-функции и их зависимость от факторов окружения. Этими факторами могут быть поставщики, люди, другие *бизнес-процессы*, услуги и т.д. *BIA* определяет последствия потери услуг для бизнеса. Потери могут быть значительными, например, крупные финансовые потери, и "мягкими" - моральные потери, потеря репутации, конкурентного преимущества и т.п.

***Анализ* влияния на бизнес определяет:**

- Форму, которую может приобретать разрушение или потеря, например:
  - Потерянный доход;
  - Дополнительные затраты;
  - Вред репутации;
  - Потеря благосклонности клиентов;
  - Потеря конкурентного преимущества;
  - Повреждение и нарушение здоровья, законности и безопасности;
  - Риск *безопасности персонала*;
  - Потеря рынка сбыта в краткосрочном и долгосрочном периодах;
  - Потеря операционных возможностей, например, контроля.
- Как будут увеличиваться негативные последствия разрушения или потери после неблагоприятного события, а также время суток, недели, месяца, когда они будут наиболее серьезными;
- Кадровое обеспечение, навыки, аппаратура и услуги, которые необходимы для поддержки минимальных уровней непрерывности критичных бизнес-процессов;
- Временные рамки, в пределах которых необходимо обеспечить минимальный уровень восстановления кадрового обеспечения, аппаратуры, услуг и других возможностей;
- Временные рамки, в пределах которых необходимо полностью восстановить критичные бизнес-процессы и поддерживающие их кадровое обеспечение, аппаратуру, услуги и другие возможности;
- Приоритеты восстановления для услуг.



Одним из основных выходов *BIA* является построение диаграммы оценки влияния потери услуги или бизнес-процесса на бизнес в целом (рис. 6.2).

Рис. 6.2. Графическое представление влияния на бизнес

Анализ влияния на бизнес предоставляет *базис* для осуществления ITSCM. На основе анализа формируется перечень услуг, приложений и других компонентов, которые станут предметами рассмотрения ITSCM.

Второй этап определения требований для ITSCM заключается в оценке вероятности возникновения неприятных событий.

Оценка рисков (Risk Assessment) - начальные шаги Управления рисками. Анализируется ценность активов для бизнеса, идентифицируются угрозы по отношению к этим активам, и оценивается *уязвимость* активов по отношению к этим угрозам[1].

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

- Принципы M_o_R - базируются на принципах управления организацией и являются необходимыми для эффективного управления рисками;
- Подход M_o_R - подход организации к указанным выше принципам должен быть отображен в ряде документов, в частности, в Политике управления рисками.
- Процессы M_o_R. Выделяют четыре процесса в рамках M_o_R:
  - Определение - определение угроз для деятельности, которые могут повлиять на достижение ею намеченного результата;
  - Оценка - оценка суммарного влияния всех определенных угроз;
  - Планирование - определение набора управленческих действий, которые уменьшат риски;
  - Реализация - осуществление запланированных управленческих действий, их контроль, определение эффективности и корректирование в случае необходимости.
- Пересмотр и внедрение M_o_R - внедрение процессов, политик и подхода M_o_R так, чтобы они непрерывно контролировались и оставались эффективными;
- Взаимодействие - обеспечение взаимодействия всех действий в рамках M_o_R с целью поддержки актуальности информации об угрозах, возможностях и других аспектах Управления рисками.

Действия в рамках ITSCM должны быть направлены на уменьшение влияния рисков и вероятности их возникновения.

Результаты Анализа влияния на бизнес и Оценки рисков являются основой для построения Стратегии непрерывности услуг в соответствии с потребностями бизнеса. Большинство организаций должны соблюдать баланс уменьшения рисков и формирования механизмов восстановления. Как бы хорошо ни проводились действия по уменьшению рисков, невозможно исключить их все. Поэтому всегда необходимо внедрять *механизмы* восстановления в интеграции с процессом Управления доступностью, так как именно доступность услуг пострадает в первую *очередь* при возникновении неприятных для бизнеса событий. Типичные меры уменьшения рисков включают в себя:

- Инсталляция UPS и резервного питания для компьютеров;
- Обеспечение отказоустойчивости систем с критичными приложениями, для которых неприемлем любой простой (например, банковская система);
- Использование RAID и зеркальных дисков для серверов для избегания потери информации и обеспечения непрерывности работы;

- Наличие запасных компонентов/оборудования, которые будут использованы в случае сбоя основных. Например, запасной сервер с минимально необходимой конфигурацией, который будет задействован в кратчайшее время в случае отказа основного сервера;
- Устранение spofов, например, единой точки доступа в сеть или единой точки электропитания.
- Использование надежных IT-систем и сетей;
- Аутсорсинг услуг нескольким поставщикам услуг;
- Увеличение контроля над безопасностью;
- Увеличение контроля над *обнаружением нарушений* в работе услуг;
- Всеобъемлющая стратегия восстановления и резервного копирования, включающая в себя внешнее хранение. Внешнее хранение предполагает регулярное (чаще всего ежедневное) копирование критичной информации во внешнее хранилище.

Перечисленные выше меры не решат всех вопросов ITSCM, но их использование позволит сильно сократить риск потерь для бизнеса в случае возникновения непредвиденных обстоятельств.

Опции восстановления в рамках ITSCM, которые должны быть учтены при формировании стратегии:

- **Переход на ручную работу** для некоторых типов услуг может стать хорошей альтернативой на короткий период до восстановления услуги. Например, Сервис-деск может работать какое-то время с бумажными заявками и журналами;
- **Взаимные соглашения** являются еще одной опцией для восстановления. Предполагают заключение соглашений между организациями, использующими похожие технологии. В настоящее время являются неприемлемыми для большинства IT-систем, но могут использоваться в отдельных случаях - например, для внешнего резервного копирования или использования принтеров;
- **Постепенное восстановление (Gradual Recovery)** - способ восстановления, также известный как "холодное резервирование". Предусматривается восстановление услуги в течение более чем 72 часов. При постепенном восстановлении обычно задействован мобильный или стационарный резервный центр, оснащенный элементами жизнеобеспечения и сетевой разводкой, без компьютерных систем. Эта опция восстановления рекомендована для некритичных услуг, предоставление которых может быть задержано на дни и недели без значительного влияния на бизнес;
- **Промежуточное восстановление (Intermediate Recovery**) - способ восстановления, также известный как "теплое резервирование". Предусматривается восстановление услуги в течение 24 - 72 часов. При промежуточном восстановлении обычно используется общий мобильный или стационарный резервный центр, оснащенный компьютерными системами и сетевыми компонентами. Конфигурирование аппаратного и программного обеспечения, а также восстановление данных выполняются в рамках Плана обеспечения непрерывности услуг. Данная опция восстановления обычно предлагается третьими сторонами, которые имеют для этого все необходимое оборудование и квалифицированный персонал. Стоимость этой опции восстановления зависит от ресурсов третьей стороны, которые должны быть задействованы для восстановления, а также от времени, в течение которого требуется восстановить услугу. Преимуществом данного метода является его прозрачность для пользователей. Недостатком - то, что информация (в том числе конфиденциальная) будет храниться у сторонней организации. Последнее делает неприемлемым данный способ восстановления для многих организаций.

- **Быстрое восстановление (Fast Recovery)** - способ восстановления. Предусматривается восстановление услуги за короткий промежуток времени, обычно менее 24 часов. При быстром восстановлении обычно используется выделенный стационарный резервный центр с компьютерными системами и ПО, сконфигурированными для работы услуг. Немедленное восстановление может занимать до 24 часов, если требуется восстановление данных резервного копирования.
- **Немедленное восстановление (Immediate recovery)** - способ восстановления, также известный как "горячее резервирование". Предусматривается восстановление услуги без прерывания услуги. Немедленное восстановление обычно использует технологии зеркалирования, балансировки загрузки и разделения площадок установки оборудования. Этот способ чаще всего предусматривает "двойную локацию" компонентов системы, то есть полное дублирование. Он является самым дорогим и применяется только для критичных бизнес-процессов, простой которых может оказать значительное негативное влияние на бизнес. Копии должны быть расположены на максимальном удалении от оригиналов, чтобы не быть задетыми разрушающим событием.

Стратегия обеспечения непрерывности должна включать в себя все рассмотренные выше способы восстановления. Различные услуги, используемые организацией, требуют различных подходов к восстановлению и уменьшению рисков сбоя. Какая бы *опция* ни выбиралась, она должна быть экономически эффективной. Главное правило - чем дольше бизнес может обходиться без услуги, тем дешевле должно быть решение по обеспечению ее непрерывности.

Стадия 3 - Реализация

После того, как Стратегия обеспечения непрерывности определена, необходимо разработать Планы обеспечения непрерывности услуг в соответствии с Планами обеспечения непрерывности бизнеса. Планы ITSCM должны рассматривать все действия, которые необходимо предпринять для предоставления требуемых услуг, возможностей и ресурсов с соответствующими уровнями непрерывности. Это значит не только рассмотрение вопросов, связанных с восстановлением услуг и возможностей, но и понимание зависимостей между ними, тестирование, проверка целостности и последовательности данных. Планы ITSCM также должны включать документацию о средствах обеспечения надежности и мерах восстановления, обоснование применения конкретных мер в зависимости от ситуации. При формировании планов необходимо убедиться в том, что в них детально рассмотрены и документированы все действия по восстановлению в случае сбоя. Планы *ITSCM* должны включать в себя такие основные моменты как точка восстановления данных, перечень зависимых систем, природа этой зависимости, требования к программному и аппаратному обеспечению, конфигурационные детали и другую важную информацию о системах и услугах.

Одним из наиболее важных источников информации для формирования планов является *Анализ* влияния на бизнес. Другие области также должны быть проанализированы: *SLA*, *требования безопасности*, инструкции эксплуатации, процедуры, внешние контракты.

Помимо разработки Планов обеспечения непрерывности для того, чтобы следовать принятой Стратегии обеспечения непрерывности, необходимы следующие действия:

1. Планирование организационной структуры

В случае возникновения катастрофы, организационная структура вероятнее всего претерпит изменения и будет основана, прежде всего, на следующем:

- Руководство - топ-менеджеры и правление организации, которые обладают властью и средствами контроля над организацией. Именно руководство ответственно за управление в кризисной ситуации;
- Координация - уровень, ответственный за координацию внутри процесса восстановления;
- Восстановление - совокупность групп бизнеса и IT, которые представляют критичные бизнес-функции и услуги, поддерживающие эти функции. Каждая группа ответственна за исполнение планов восстановления своей области при взаимодействии с персоналом, пользователями и третьими сторонами.

2. Тестирование

Планы по восстановлению должны пройти тестирование. Тестирование является важной частью ITSCM. Именно оно гарантирует то, что принятые стратегия, соглашения, планы и процедуры будут действительно работать на практике.

Поставщик услуг ответственен за то, что в случае катастрофы услуги могут быть восстановлены в заданный временной *интервал* с требуемой функциональностью и производительностью. Тесты должны проводиться по максимально реалистичным сценариям. Тем не менее, необходимо понимать, что даже самое тщательное тестирование не может учесть все нюансы, которые могут возникнуть в реальности.

Стадия 4 - Непрерывная *эксплуатация*

Эта стадия состоит из следующего:

1. Обучение, готовность, тренинги - персонал должен быть готов к возникновению непредвиденных обстоятельств и знать, что необходимо делать при их возникновении;
2. Пересмотр - все выходы процесса ITSCM должны регулярно пересматриваться на предмет актуальности и корректироваться в случае необходимости;
3. Тестирование - помимо начального тестирования, необходимо предусмотреть регулярное тестирование стратегии, планов и других выходов ITSCM. Резервные копии и механизмы восстановления также должны тестироваться;
4. Управление изменениями - процесс, ответственный за оценку изменений с точки зрения их влияния на планы ITSCM.

Инициирование является заключительным тестом для Планов обеспечения непрерывности бизнеса и услуг. Этот процесс должен рассматривать процедуру запуска планов по восстановлению в случае непредвиденных обстоятельств. Необходимо помнить, что решение об инициации планов должно быть хорошо взвешенным, особенно в случае использования услуг восстановления третьих сторон. Сбой может произойти в любое время дня и ночи, поэтому важно иметь возможность незамедлительно инициировать планы по восстановлению.

Входами ITSCM являются:

1. Информация от бизнеса - стратегия, планы и бюджет организации, текущие и будущие требования;
2. Информация от IT - стратегия, планы и бюджет IT;
3. Стратегия и планы обеспечения непрерывности бизнеса;
4. Информация об услугах - информация от *SLM*, в частности из портфеля услуг и каталога услуг, SLA/*SLR*;

5. Финансовая информация - информация от процесса управления финансами о стоимости предоставления услуг, ресурсов и компонентов;
6. Информация об изменениях - информация от процесса управления изменениями, в частности расписание изменений и их влияние на планы обеспечения непрерывности;
7. Информация о взаимоотношениях бизнеса с услугами, вспомогательными услугами и технологиями.
8. Расписания управления непрерывностью бизнеса и управления доступностью;
9. Планы обеспечения непрерывности услуг и отчеты тестирования партнеров, поставщиков.

Выходами ITSCM являются:

1. Политика и стратегия ITSCM;
2. Набор планов, в том числе планы Антикризисного управления, Срочных ответных действий, Восстановления после катастрофы, а также совокупность вспомогательных планов и контрактов с поставщиками услуг по восстановлению.

Антикризисное управление (Crisis Management) - *процесс, отвечающий за управление непрерывностью бизнеса в самом широком смысле. Команда антикризисного управления отвечает за стратегические вопросы, такие как управление взаимодействием со средствами массовой информации и доверием акционеров, а также принимает решение об инициации планов обеспечения непрерывности бизнеса.*

3. Анализ влияния на бизнес и соответствующие отчеты;
4. Анализ рисков и управленческие обзоры и отчеты;
5. Расписание тестирования ITSCM;
6. Сценарии для проведения тестирования;
7. Обзоры и отчеты по тестированию ITSCM.

Ключевым показателем производительности ITSCM является то, что предоставляемые услуги могут быть восстановлены с целью поддержки бизнеса в достижении поставленных целей:

1. Проводится регулярный аудит планов ITSCM с целью проверки того, что требования бизнеса к восстановлению могут быть удовлетворены;
2. Все целевые показатели восстановления услуг документированы, согласованы в SLA и могут быть достигнуты с помощью планов ITSCM;
3. Проводится регулярное и всеобъемлющее тестирование планов ITSCM;
4. Заключены все необходимые для ITSCM контракты с третьими сторонами;
5. Обеспечивается уменьшение рисков и негативного влияния сбоев услуг.

В качестве показателя эффективности может также выступать готовность организации к действиям в соответствии с планами ITSCM.

Основными рисками для ITSCM являются недостаточность и некорректность информации, поступающей от бизнеса, IT и других процессов, а также нехватка ресурсов для обеспечения непрерывности.

Главный источник рисков при этом - отсутствии процесса BCM в компании!!!