СТАНДАРТ COBIT
УПРАВЛЕНИЕ И АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ. ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНЕШНЕГО АУДИТА ИТ

Сергей Гузик

Управление ИТ — составная часть успеха в управлении предприятием, которая гарантирует рациональное и эффективное совершенствование всех взаимосвязанных процессов предприятия. Управление ИТ предоставляет основу, которая связывает ИТ-процессы, ИТ-ресурсы и информацию со стратегией и целями организации, что позволяет максимально эффективно использовать информацию, повышая капитализацию и получая конкурентоспособные преимущества.

Принципы управления созданы для того, чтобы помочь руководителю ИТ ответить на три стратегических вопроса:

1. Существуют ли в настоящее время в организации Информационные Технологии, при управлении которыми "удовлетворяются" все информационные потребности организации?
2. Как организация обеспечивает инфраструктуру и управляет рисками, насколько организация зависит от этого?
3. С какими проблемами организация сталкивается при управлении ИТ?

Чтобы получить ответы на эти стратегические вопросы необходимо непрерывно отвечать на "тактические" вопросы:

- Что является результатом ИТ-процессов?
- Что является решением проблем в ИТ?
- Из чего состоят эти решения?
- Будут ли работать эти решения?
- Как их реализовать?

Для получения ответов на "тактические" вопросы в книге Принципы управления CobiT, включены Модели Зрелости, Критические Факторы Успеха (КФУ), Ключевые Индикаторы Цели (КИЦ) и Ключевые Показатели Результата (КПР), это дополнение позволило получить качественно улучшенный подход к вопросам управления ИТ, который отвечает потребностям руководителей в части управления и контроля. Предоставляя руководителю организации инструмент управления и измерения ИТ на соответствие тридцати четырем ИТ-процессам, определенным в CobiT.

Для информационной поддержки принятия решений, в книге Принципы управления описаны следующие виды представления информации:

1. Инструментальная панель;
2. Карты оценки;
3. Эталонное тестирование.

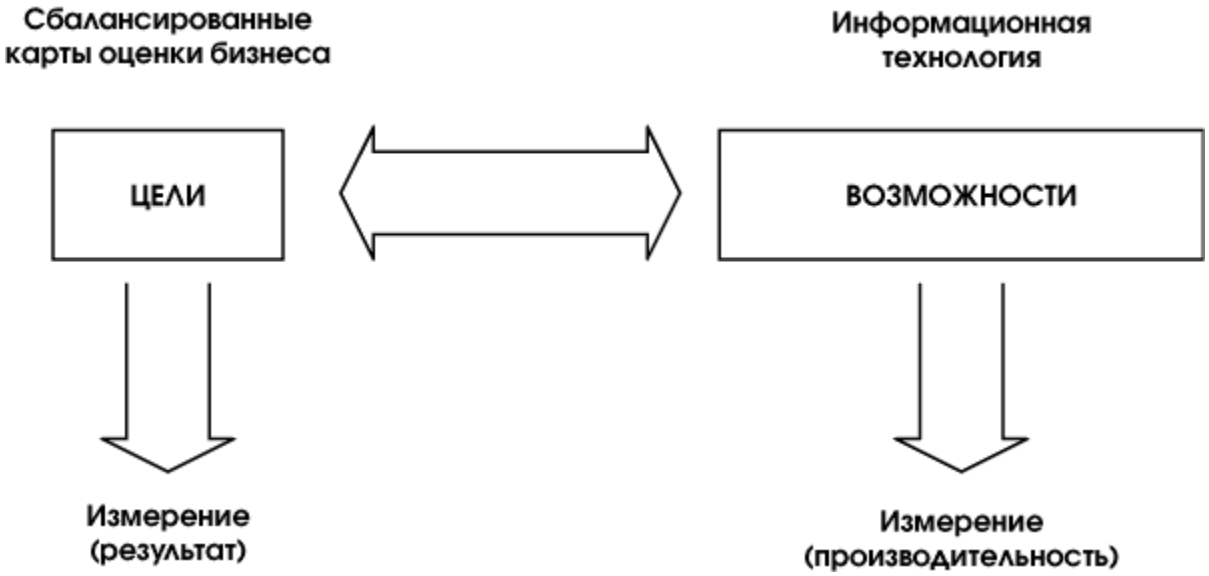
Первой целью **Принципов управления** CobiT явилось создание индикаторов для инструментальной панели, единиц измерения для карт оценки, шкал сравнения для эталонного тестирования.

Необходимость "измерения" процессов организации обусловлена важностью непрерывного совершенствования ИТ, что создает потребность в комплекте инструментов для контроля. При этом трудно определить необходимый уровень совершенствования и остановиться на нем. Перед руководителями в коммерческих и некоммерческих организациях часто возникают задачи оценить объемы инвестиций в ИТ и инфраструктуру, при этом далеко не все могут обосновать инвестиции, отвечая на вопрос:

"Как далеко необходимо зайти, и будут ли оправданы затраты выгодой?". **Принципы управления** CobiT призваны ответить на этот вопрос и помочь в обосновании инвестиций в ИТ.

В настоящее время информационные услуги преобладают над прочими поддерживающими бизнес услугами. Таким образом, ИТ становятся одним из первостепенных показателей бизнеса. Как следствие — отношения между бизнес-целями с их единицами измерения и ИТ с его целями и единицами измерения являются очень важными и могут быть изображены следующим образом (Рис. 6).

Рисунок 6. Схема отношения бизнес целей и ИТ



Создание такой взаимной связи поможет руководителям в контроле над информационными технологиями организации, отвечая на следующие вопросы:

1. О чем беспокоится руководство организации? Необходимо удостовериться, что выполняются все потребности организации.
2. Где измеряется удовлетворение потребностей? Результат бизнес-процесса представлен на сбалансированной карте оценок бизнеса как Ключевой Индикатор Цели.
3. Затрагивают ли проблемы, возникающие в ходе реализации бизнес-процессов, информационные технологии организации? ИТ-процессы своевременно предоставляют организации правильную информацию, позволяя ее бизнес-процессам эффективно и бесперебойно функционировать. Это является Критическим Фактором Успеха для организации.
4. Где это измеряется? Ключевой Индикатор Цели, основанный на сбалансированной карте оценки, представляет ИТ-информацию, сопоставимую с критериями информации (Эффективность, Продуктивность, Конфиденциальность, Целостность, Пригодность, Согласованность, Надежность).
5. Что еще должно быть измерено? Если ответы на первые вопросы — положительные, должно быть учтено влияние множества Критических Факторов Успеха, которые должны быть измерены как Ключевые Индикаторы Результата для ИТ-процессов.

Модели зрелости

Модели зрелости в CobiT предназначены для контроля над ИТ-процессами организации. Они базируются на определении уровня развития организации от несуществующего до оптимизированного (от 0 до 5 уровня модели зрелости). Этот подход был привнесен в CobiT из Моделей Зрелости, разработанных Институтом проектирования

и разработки программного обеспечения (Software Engineering Institute), созданных для оценки уровня зрелости разработки программного обеспечения.

Ответом на вопрос "чем и как управлять" явилась разработка моделей зрелости, начатая в конце 80-х годов Институтом проектирования и разработки программного обеспечения (Software Engineering Institute's), по заказу Министерства обороны США. Первоначальное предназначение — создание эффективного инструмента для классификации и оценки проектов, связанных с разработкой программного обеспечения и гарантированного соблюдения качества при выполнении этих проектов. В дальнейшем модели зрелости были доработаны для управления ИТ-сервисами и аудита процессов управления.

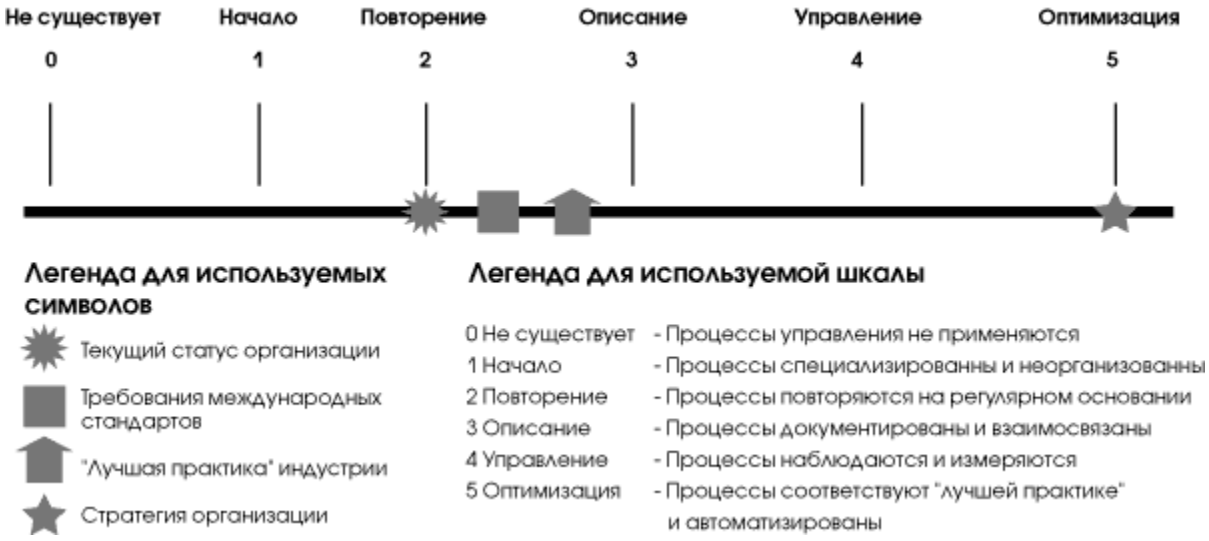
Maturity Models (ММ) — "модели зрелости". Соответствие уровням "модели зрелости" означает, что компания готова к плановой модернизации или обновлению. ММ — не технология, не стандарт, для нее нет формальных описаний, в ней нет жестких требований, и она не привязана к конкретным информационным технологиям.

Модели зрелости не подсказывают как улучшить работу компании и не объясняют, как работать с персоналом, также нет готовых руководств и по применению моделей зрелости. Рекомендуется каждой конкретной компании разработать подобное руководство для своего бизнеса или пригласить сторонних консультантов для решения этого вопроса. Модели зрелости предназначены для организации эффективного управления. Они определяют ключевые действия, которые указывают, что надо сделать для достижения требуемого качества и содержат способы контроля над правильностью выполнения ключевых ИТ-процессов и методы их корректировки. Ключевые действия подробно описаны в Руководстве на абстрактном уровне, а в процессе использования ММ компания может выбрать произвольную степень их формализации.

Беря за основу шкалу моделей зрелости (Рис. 7), разработанную для каждого из 34 ИТ-процесса CobiT, руководитель может выяснить следующие сведения:

- Текущий статус организации — оценить, на какой стадии организация находится сегодня.
- Текущий статус лучшей практики в этой отрасли — сравнить свою организацию с лучшей организацией в этой отрасли.
- Текущий статус международных стандартов — провести дополнительное сравнение текущего статуса организации с "лучшей практикой" или международными стандартами.
- Статус организации после усовершенствования (реализация стратегии организации) — оценить стратегию организации, каких результатов организация хочет достичь.

Рисунок 7. Шкала моделей зрелости



Модель Зрелости Управления ИТ, для бизнеса, предназначена для управления ИТ-процессами с целью увеличения ценности ИТ, при соблюдении равновесия между риском и прибылью.

- **0. Не существует.** Полное отсутствие каких-либо процессов управления ИТ. Организация не признает существования проблем в ИТ, которые нужно решать, и, таким образом, нет никаких сведений о проблемах.
- **1. Начало (Анархия).** Организация признает существование проблем управления ИТ и необходимость их решения. При этом не существует никаких стандартизованных решений. Существуют случайные одномоментные решения, принимаемые кем-то персонально или от случая к случаю. Подход руководства к решению ИТ-проблем хаотичен, признание существования проблем случайно и непоследовательно.
- **2. Повторение (Фольклор).** Существует всеобщее осознание проблем управления ИТ. Показатели деятельности и ИТ-процессов находятся в развитии, охватывая процессы планирования, функционирования и мониторинга ИТ. Деятельность по управлению информационными технологиями описана и интегрирована в процесс управления организацией. Выбраны для улучшения и/или контроля те ИТ-процессы, которые влияют на основные бизнес-процессы предприятия. Эффективно выполняется планирование и управление инвестициями. Руководство организации регламентировало меры по управлению ИТ, а также методы управления и оценки, но процесс не был принят в организации. Не существует формализованного обучения, набора взаимосвязанных стандартных процедур управления, ответственность возложена на сотрудников. Сотрудники контролируют процессы управления с помощью проектов и ИТ-процессов. Ограниченные инструменты управления выбираются и внедряются для сбора метрик управления, но не используются в полном объеме из-за недостатков в оценке их функциональности.
- **3. Описание (Стандарты).** Необходимость действовать в соответствии с принципами управления ИТ понимается и принимается. Развивается базовый набор показателей управления ИТ: определена связь между результатом и показателями производительности, она зафиксирована и внедрена в стратегические процессы планирования и мониторинга. Процедуры стандартизованы и документированы, проводится обучение сотрудников по выполнению этих процедур. Показатели производительности всех видов деятельности зафиксированы и отслеживаются, что приводит к повышению эффективности работы всей организации. Процедуры не сложны, они являются формализацией существующей практики. Идеи сбалансированных карт оценки бизнеса принимаются организацией. Ответственность за обучение, выполнение и применение стандартов возложена на сотрудников организации. Анализ первопричин применяется время-от-времени. Большинство процессов управляются в соответствии с некоторыми основными метриками, и, как правило, отдельными сотрудниками, поэтому ни о каких отклонениях руководители не знают. Однако всеобщая отчетность о выполнении ключевых процессов является четкой, и руководство премирует сотрудников на основе измерения ключевых результатов.
- **4. Управление (Измеряемый).** Существует полное понимание проблем управления ИТ на всех уровнях организации, постоянно происходит обучение сотрудников. Определены и поддерживаются в актуальном состоянии соглашения об уровне обслуживания. Четко распределена ответственность, установлен уровень владения процессами. Процессы ИТ соответствуют бизнесу и стратегии ИТ. В первую очередь улучшения в процессах ИТ основываются на измеряемых количественных показателях. Существует возможность управлять процедурами и метриками процессов, измерять их соответствие. Все совладельцы процесса осознают риски, важность ИТ и возможности, которые они предоставляют. Руководство организации определило допустимые отклонения, при которых процессы должны работать. Если процессы не работают эффективно и продуктивно, действия предпринимаются во многих (но не всех случаях). Процессы постоянно совершенствуются, их результаты соответствуют "лучшим практикам". Формализован порядок анализа первопричин. Присутствует понимание необходимости постоянного совершенствования. Ограниченно применяются передовые технологии, основанные на современной инфраструктуре и модифицированных стандартных инструментах. Все необходимые ИТ-специалисты вовлечены в бизнес-процессы.

Управление ИТ превращается в процесс уровня всей организации. Деятельность управления ИТ интегрируется в процесс управления организацией.

- **5. Оптимизация (Оптимизируемый).** В организации существует углубленное понимание управления ИТ, проблем и решений ИТ, а также перспектив. Обучение и коммуникация поддерживаются на должном уровне, самыми современными средствами. В результате непрерывного улучшения процессы соответствуют моделям зрелости, построенным на основании "лучшей практики". Внедрение этих процедур привело к появлению организаций, людей и процессов, максимально адаптируемых к изменяющимся условиям, а также полностью соответствующих требованиям управления ИТ. Первопричины всех проблем и отклонений тщательно анализируются, по результатам анализа выполняются результативные действия. Информационные технологии интегрированы в бизнес-процессы, полностью их автоматизируют, предоставляя возможность повышать качество и эффективность работы организации.

Критические Факторы Успеха (КФУ)

Критические Факторы Успеха (КФУ) — определяют наиболее важные проблемы или действия руководителей, направленные на достижение контроля над ИТ-процессами. КФУ должны быть управляемыми, ориентированными на успех и описывать, как выполнять необходимые стратегические, технические, организационные или процедурные действия для достижения успеха.

Примеры Критических Факторов Успеха (КФУ):

- Действия по управлению ИТ интегрированы в процессы управления организации и стиль работы руководителей;
- Управление ИТ сосредоточенно на целях организации: стратегических инициативах, использовании технологий для развития бизнеса, достаточности ресурсов и удовлетворения бизнес-требований;
- Действия по управлению ИТ ясно определены, формализованы и осуществляются на основе потребностей предприятия с соответствующей отчетностью;
- Методы управления разработаны для увеличения продуктивности, оптимального использования ресурсов и увеличения эффективности ИТ-процессов;
- Организационные методы следят за окружающей средой и культурой управления; способствуют нормальному контролю; ведению стандартной практики управления рисками; определяют степень соответствия установленным стандартам; управляют и изучают недостатки и риски;
- Методы аудита определены таким образом, чтобы избежать сбоев и ошибок в системе внутреннего контроля;
- Наблюдается интеграция и развитие взаимодействия сложных ИТ-процессов, таких как управление проблемами, изменениями и конфигурациями;
- Учрежден контрольный комитет, назначающий и наблюдающий за независимым аудитом, уделяющий пристальное внимание ИТ при составлении планов аудита, а также принимающий во внимание результаты исследований сторонних организаций и аудиторов.

Ключевые Индикаторы Цели (КИЦ)

Ключевые Индикаторы Цели (КИЦ) описывают комплекс измерений, которые по факту сообщают руководству, что ИТ-процесс достиг предъявляемых бизнес-требований. КИЦ выражается в терминах информационных критериев:

- Пригодность информации, необходимой для поддержки бизнеса;
- Риски отсутствия целостности и конфиденциальности;
- Рентабельность процессов и операций;
- Подтверждение надежности, эффективности и согласованности.

Ключевыми Индикаторами Цели (КИЦ), могут быть:

- Улучшение управления производительностью и стоимостью;
- Увеличение дохода от инвестиций в ИТ;
- Сокращение времени запуска в продажу нового продукта или услуги;
- Улучшение управления качеством, новшествами и рисками;
- Соответствующая интеграция и стандартизация бизнес-процессов;
- Поиск новых и удовлетворение существующих клиентов;
- Выполнение требований и ожиданий клиента по бюджету и времени;
- Соответствие законам, инструкциям, промышленным стандартам и договорным обязательствам;
- Полное осознание меры принимаемого риска, а также соответствие уровню риска, приемлемого для данной организации;
- Эталонное тестирование зрелости управления ИТ.

Ключевые Индикаторы Результата (КИР)

Ключевые Индикаторы Результата (КИР) описывают комплекс действий, необходимых для определения, насколько ИТ-процессы достигают поставленных целей. КИР являются основными индикаторами, отображающими вероятность достижения цели. А также индикаторами, отражающими адекватность способов, методов и навыков, используемых при достижении результата.

Ключевыми Индикаторами Результата (КИР), могут быть:

- Увеличение рентабельности ИТ-процессов;
- Улучшение работы и планирования действий по совершенствованию ИТ-процессов;
- Увеличение нагрузки на ИТ-инфраструктуру;
- Повышение степени удовлетворения пользователей (опросы пользователей и количество жалоб);
- Улучшение взаимодействия и коммуникаций между руководителями ИТ и руководством организации
- Повышение производительности сотрудников (в том числе, повышение морального духа).

Обобщая вышеизложенную информацию, можно сказать следующее:

- Модели зрелости предназначены для стратегического выбора и эталонного сравнения.
- Критические Факторы Успеха (КФУ) предназначены для организации контроля ИТ-процессов.
- Ключевые Индикаторы Цели (КИЦ) предназначены для контроля достижения целей ИТ-процессов.
- Ключевые Индикаторы Результата (КИР) предназначены для контроля результатов каждого ИТ-процесса.

При возрастании роли электронного бизнеса и зависимости от информационных технологий, организации должны стремиться к увеличению статуса организации, связанного, в том числе, с повышением уровней управления и безопасности ИТ. Каждая организация должна знать свои бизнес-процессы и должна отслеживать их совершенствование. Один из путей достижения конкурентоспособного уровня управления и безопасности ИТ — это эталонное тестирование и измерение совершенствования управления ИТ по сравнению с другими организациями отрасли и стратегией организации. Принципы управления CobiT предоставляют руководителю инструмент управления ИТ, позволяя отвечать на бесконечный вопрос: "Какой уровень управления необходим ИТ- организации, насколько он соответствует целям организации?"

Управление ИТ по CobiT

1. Управление ИТ осуществляется с учетом бизнес-потребностей.
2. Для управления ИТ определены информационные критерии.

Потребности бизнеса определяются Ключевыми Индикаторами Цели, чему способствует организация постоянного контроля над всеми ресурсами ИТ. Достижение необходимого уровня контроля измеряется Ключевыми Показателями Результата, которые учитывают Критические Факторы Успеха.

Модель Зрелости используется для оценки уровня управления ИТ в данной организации — от несуществующего (самый низкий уровень) до оптимизированного (самый высокий уровень).

Для достижения пятого, "оптимизированного" уровня зрелости в управлении ИТ организация должна быть, по крайней мере, на пятом уровне в домене мониторинг и как минимум на четвертом уровне моделей зрелости для всех других доменов.

В **Принципах Управления** CobiT сосредоточено краткое описание Критических Факторов Успеха, Ключевых Индикаторов Цели и Ключевых Индикаторов Результата для каждого ИТ-процесса, дополняя общий подход к управлению ИТ, изложенный в **Структуре CobiT**.