Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 1 (116)/2003

Стандарт CobiT

КОРПОРАТИВНЫЕ СИСТЕМЫ

Стандарт CobiT

Управление и аудит информационных технологий. Особенности проведения внешнего аудита ИТ

Сергей Гузик
руководитель рабочей группы ISACA.ru

СОДЕРЖАНИЕ

Введение

В условиях стремительно возрастающей роли ИТ-составляющей профессиональный подход к управлению и систематическое обследование информационных технологий (ИТ) по международным стандартам позволяют компенсировать на первый взгляд невидимые, но существенные недостатки в организации производственных процессов. Построение грамотной структуры управления, создание эффективной вертикали принятия решения и системы контроля напрямую зависят от состояния информационных технологий, от их эффективности, производительности, безопасности, надежности и других не менее важных показателей.

Эффективная система управления и контроля над ИТ решает не только внутренние проблемы, но и позволяет повысить инвестиционную привлекательность организации, позиционируя ее для инвестора как «открытую» финансовую систему. С другой стороны достаточно трудно подобрать комплексное решение для таких задач. Одно из решений — внедрение стандарта CobiT, который формализует не только конкретные проекты в сфере ИТ, но и создает то ядро управления и контроля ИТ, вокруг которого выстраиваются производственные процессы организации с максимально возможным уровнем эффективности.

Управление и аудит ИТ — это нечто большее, чем традиционный термин — управление и аудит информационной безопасности, в том числе на соответствие требованиям ФАПСИ, BS7799 (ISO 17799) или другим разработанным критериям.

В той или иной форме вопросы, связанные с внутренним контролем бизнес-процессов организации, ее финансово-хозяйственной деятельности и информационными технологиями возникают постоянно. В поиске ответов на эти вопросы руководители организаций создают собственные службы внутреннего аудита, приглашаются аудиторские компании, обращаются к консультантам.

Для решения задачи, связанной с созданием собственной службы внутреннего аудита, организация на определенном этапе оценивает экономическую эффективность подобной службы, которая призвана стать дополнительным источником информации для руководителя, принимающего решения. Если служба внутреннего аудита признается экономически эффективной для организации, то она создается, если не эффективной — то приглашаются внешние консультанты или аудиторы для проведения работ.

Независимо от результатов выбора из перечисленных выше возможностей перед руководителем неоспоримо возникает еще одна проблема: необходимость выбора методологического средства, на основе которого будет построена система управления и контроля и которое будет рабочим инструментом службы внутреннего ИТ-аудита. На сегодняшний день ощутимого недостатка в стандартах нет. Такие стандарты, как ISO, ITIL и другие, уже применяются и в российской практике, более того, интерес к ним неизменно растет. Все они практически в равной степени наделены определенными преимуществами и недостатками, прежде всего из-за функциональной направленности и специфической области применения. Любому же пользователю интересен, прежде всего, комплексный подход к решению, тем более в таком объемном и многогранном вопросе, как управление и контроль ИТ. Рассмотрим более подробно одно из существующих решений — стандарт CobiT.

Вначале, несколько слов об ассоциации ISACA, которая развивает и продвигает этот стандарт.

ISACA

Ассоциация Аудита и Контроля Информационных Систем (ISACA) была основана в 1969 году для финансовых аудиторов в контроле ИТ. Ассоциация Аудита и Контроля Информационных

Систем является ведущей мировой профессиональной организацией с представительствами в более чем 100 странах мира и охватывает все уровни ИТ:

- Организации;
- Управления;
- Практического применения.

Ассоциация занимает уникальную позицию мирового лидера в области разработки и распространения стандартов по аудиту ИТ, ее стратегический альянс с другими ассоциациями и консалтинговыми компаниями в областях финансово-хозяйственной деятельности, бухгалтерского учета и аудита ИТ обеспечивает не имеющий равных уровень интеграции и соответствия требованиям владельцев бизнес-процессов.

Управление и аудит ИТ. Стандарт CobiT

Аббревиатура CobiT расшифровывается как Контрольные ОБъекты для Информационных и смежных Технологий. За этой аббревиатурой скрывается набор документов, в которых изложены принципы управления и аудита информационных технологий. CobiT позиционируется как открытый стандарт «де-факто», в настоящее время переживающий свое третье издание.

В состав стандарта входят шесть книг, ориентированных на разные аудитории:

1. **Резюме для руководителя.** Описание стандарта CobiT, ориентированное на топ-менеджеров организации для принятия ими решения о применимости стандарта в конкретной организации. С переводом этой книги на русский язык Вы можете ознакомиться: http://www.isaca.ru
2. **Описание структуры.** Книга содержит развернутое описание структуры стандарта, высокоуровневых целей контроля и пояснения к ним, необходимые для эффективной навигации и результативной работы со стандартом.

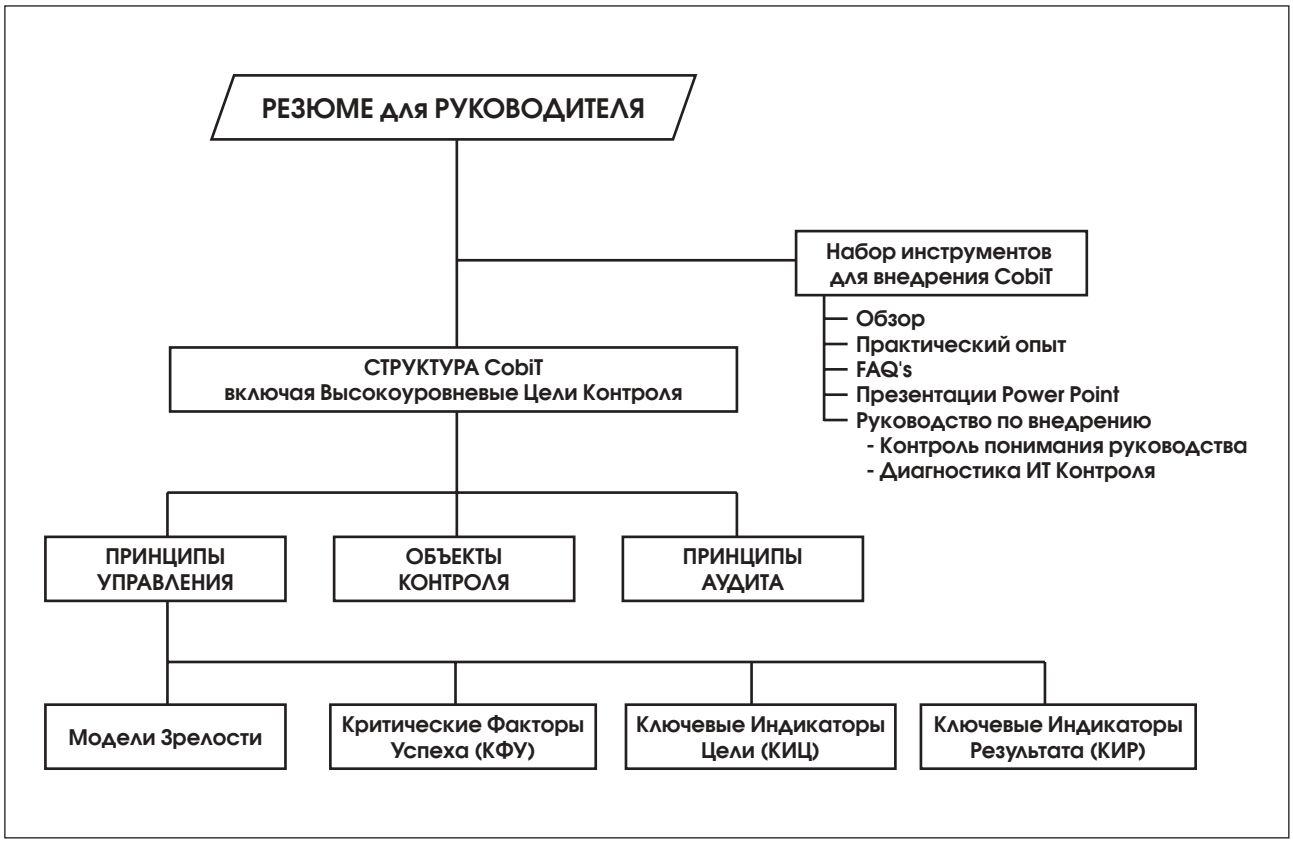


Рис. 1. Состав книг CobiT

3. **Объекты контроля.** В книгу включены детальные описания объектов контроля, содержащие расшифровку каждого из объектов.
4. **Принципы управления.** Книга отвечает на вопросы как управлять ИТ, как правильно поставить достижимую цель, как ее достичь и как проконтролировать полноту ее достижения. Предназначена для руководителей ИТ-служб.
5. **Принципы аудита.** Правила проведения ИТ-аудита. Описание того, у кого можно получить необходимую информацию, как ее проверить, какие вопросы задавать? Книга предназначена для внутренних и внешних аудиторов ИТ, а также консультантов в сфере ИТ.
6. **Набор инструментов внедрения стандарта** — практические советы по ежедневному использованию стандарта в управлении и аудите ИТ. Книга предназначена для внутренних и внешних аудиторов ИТ, консультантов в сфере ИТ.

Модель процессов, выстраиваемая на базе CobiT, предпочтительней других подходов, в основе которых не лежат бизнес-процессы организации (методики и стандарты аудита производителей программно-аппаратных средств), по нескольким причинам:

1. По определению: **процесс – это действие, направленное на достижение результата, при оптимальном использовании ресурсов, и которое может корректироваться при его выполнении.** При выполнении процесса все задействованные ресурсы структурируются и выстраиваются таким образом, чтобы максимально эффективно выполнять этот процесс.
2. Во-вторых, процессы в подавляющем большинстве организаций, а особенно их цели не так часто изменяются, по сравнению с организационными объектами (организационно-штатная структура: сотрудники, отделы, департаменты и т.д.).
3. В-третьих, развертывание информационной системы или внедрение информационных технологий не может быть ограничено спецификой одного отдела или департамента, а затрагивает руководителей, пользователей из других подразделений и ИТ-специалистов. Таким образом, прикладные системы (прикладное программное обеспечение то, что видит пользователь) — это неотъемлемая часть структуры CobiT и могут быть стандартно оценены, как и прочие объекты контроля CobiT, в рамках единой структуры и с применением единых метрик.

CobiT – это сохранение единого подхода к сбору, анализу информации, подготовке выводов и заключений на всех этапах управления, контроля и аудита ИТ, возможность сравнения существующих ИТ-процессов с «лучшими» практиками, в том числе отраслевыми.

Основа CobiT. Разделение CobiT на управление и аудит

В основу стандарта CobiT положено следующее утверждение: **для предоставления информации, необходимой организации для достижения ее целей, ресурсы ИТ должны управляться набором естественно сгруппированных процессов.**

Для этого CobiT выделяет 34 высокоуровневые цели контроля, по одной на каждый ИТ-процесс, которые сгруппированы в 4 домена:

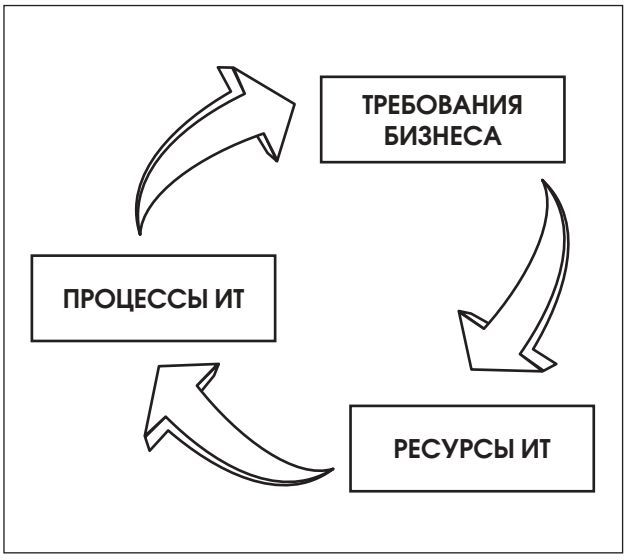


Рис. 2. Цикл CobiT, отражающий непрерывность соответствия ИТ требованиям бизнеса

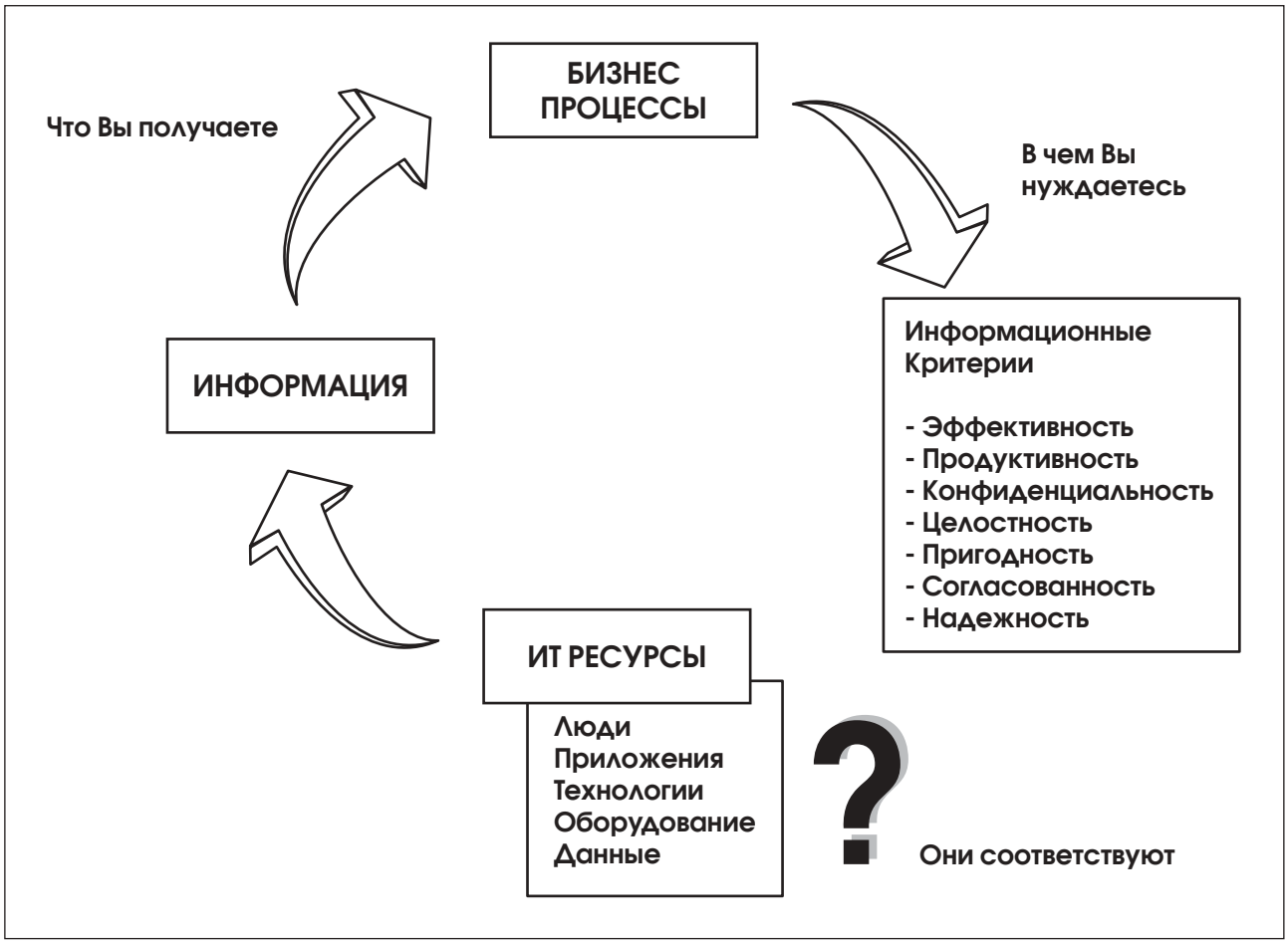


Рис. 3. Вопросы CobiT, на всем жизненном цикле ИТ

Планирование и Организация; Проектирование и Внедрение; Эксплуатация и Сопровождение; Мониторинг. Предлагаемая структура объединяет все аспекты информации и технологий, поддерживающих ее. Применяя 34 высокоуровневые цели контроля, руководитель может быть уверен, что ему будет предоставлена адекватная система контроля над ИТ-средой, которая учитывает задействованные ресурсы ИТ, дающая возможность оценить ИТ по предлагаемым CobiT семи критериям оценки информации.

Ресурсы ИТ в CobiT описаны пятью составляющими:

1. **Данные** — объекты в широком смысле (то есть внутренние и внешние), структурированные и неструктурированные, а также графика, звук и т.д.
2. **Приложения** — совокупность автоматизированных и выполняемых вручную процедур.
3. **Технология** — аппаратное обеспечение, программное обеспечение, операционные системы, системы управления базами данных, сетью и мультимедиа.
4. **Оборудование** — все ресурсы, создающие и поддерживающие информационные технологии.
5. **Люди** — персонал, его навыки: умение планировать и организовывать, комплектовать, обслуживать и контролировать информационные системы и услуги.

При этом денежные средства или капитал не рассматриваются в качестве ИТ-ресурса. Они могут рассматриваться в качестве инвестиций в любой из вышеуказанных ресурсов.

Критерии оценки информации:

- **Эффективность** — актуальность информации, соответствующего бизнес-процесса, гарантия своевременного и регулярного получения правильной информации.
- **Продуктивность** — обеспечение доступности информации с помощью оптимального (наиболее продуктивного и экономичного) использования ресурсов.
- **Конфиденциальность** — обеспечение защиты информации от неавторизованного ознакомления.

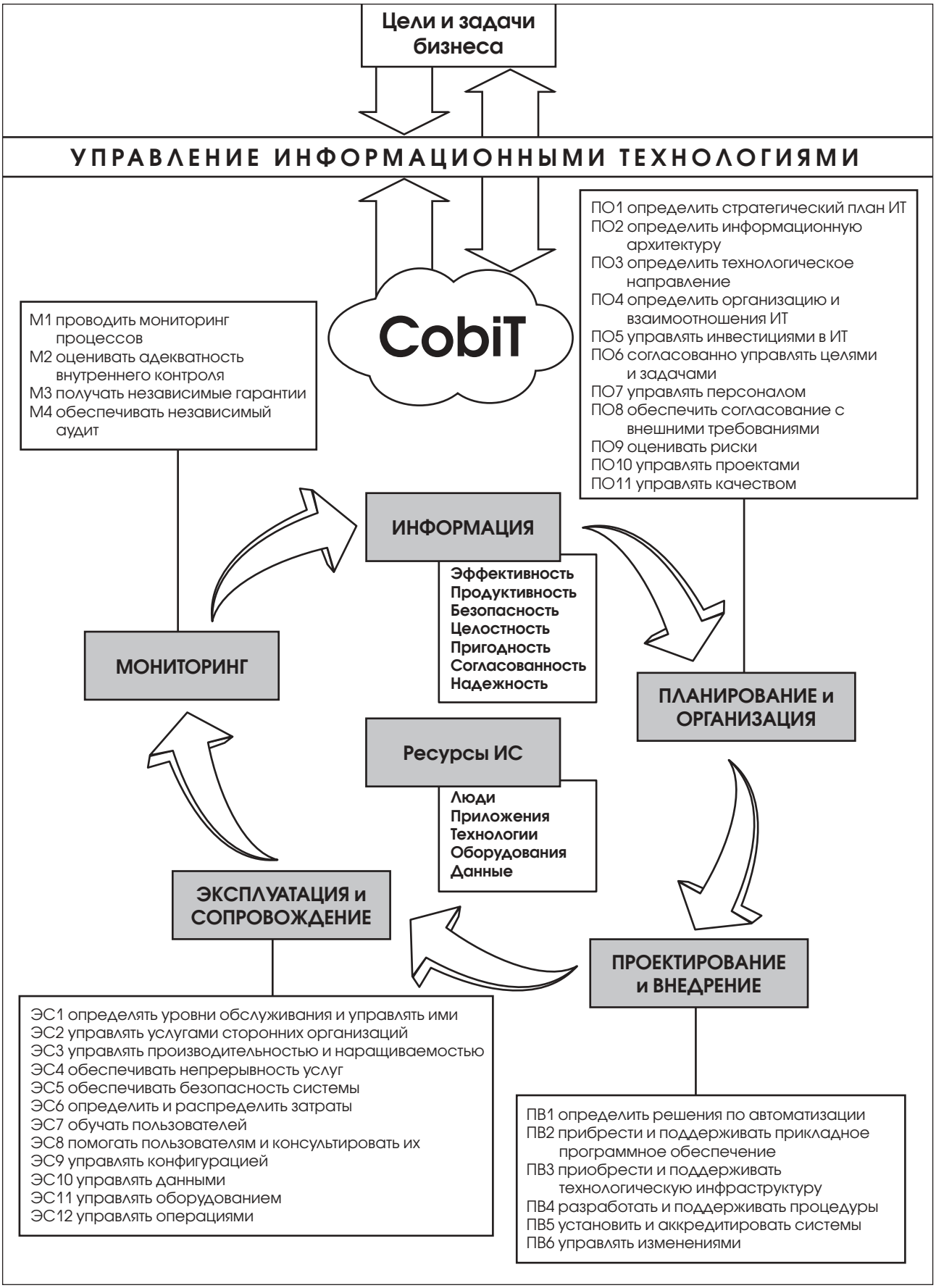


Рис. 4. Четыре домена CobiT, объединяющие 34 ИТ-процесса, критерии информации и ресурсы ИТ

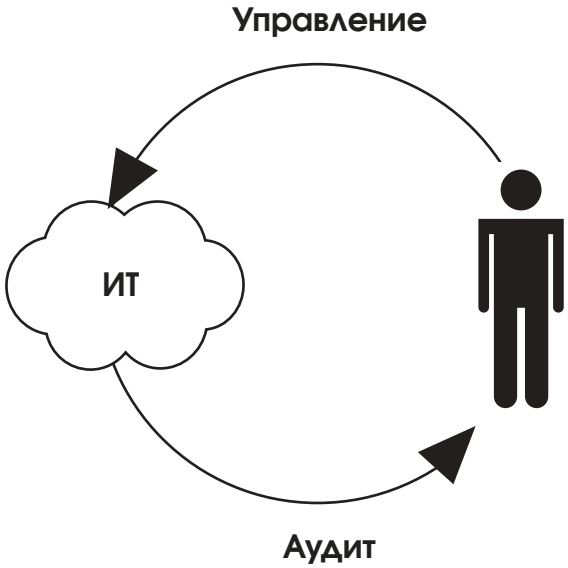
- **Целостность** — точность, полнота и достоверность информации в соответствии с требованиями бизнеса.
- **Пригодность** — предоставление информации по требованию бизнес-процессов.
- **Согласованность** — соответствие законам, правилам и договорным обязательствам.
- **Надежность** — доступ руководства организации к соответствующей информации для текущей деятельности, для создания финансовых отчетов и оценки степени соответствия.

Схема CobiT, объединяющая 34 ИТ-процесса и учитывающая критерии информации и ресурсы ИТ на всем протяжении жизненного цикла, представлена на рисунке 3.

Для достижения целей организации в сфере ИТ, CobiT включает в себя две основные книги, которые отражают **Принципы управления и Принципы аудита**.

Как следует из названия — это две части одного целого (оказание воздействия и контроль результатов). **Управляем – воздействуем на ИТ для достижения поставленных целей. Аудит – контролируем достижение цели.**

Необходимо отметить, что в основе стандарта лежат *Объекты Контроля* CobiT, именно они являются базой стандарта и объединяют все его книги, предлагая пользователю единую основу управления и аудита ИТ.



Принципы управления ИТ, стандарт CobiT

Принципы управления, книга стандарта CobiT, описывающая управление ИТ — одна из последних разработок Института Управления ИТ, пополнившая перечень книг CobiT в 3-ем издании стандарта.

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 соответ-

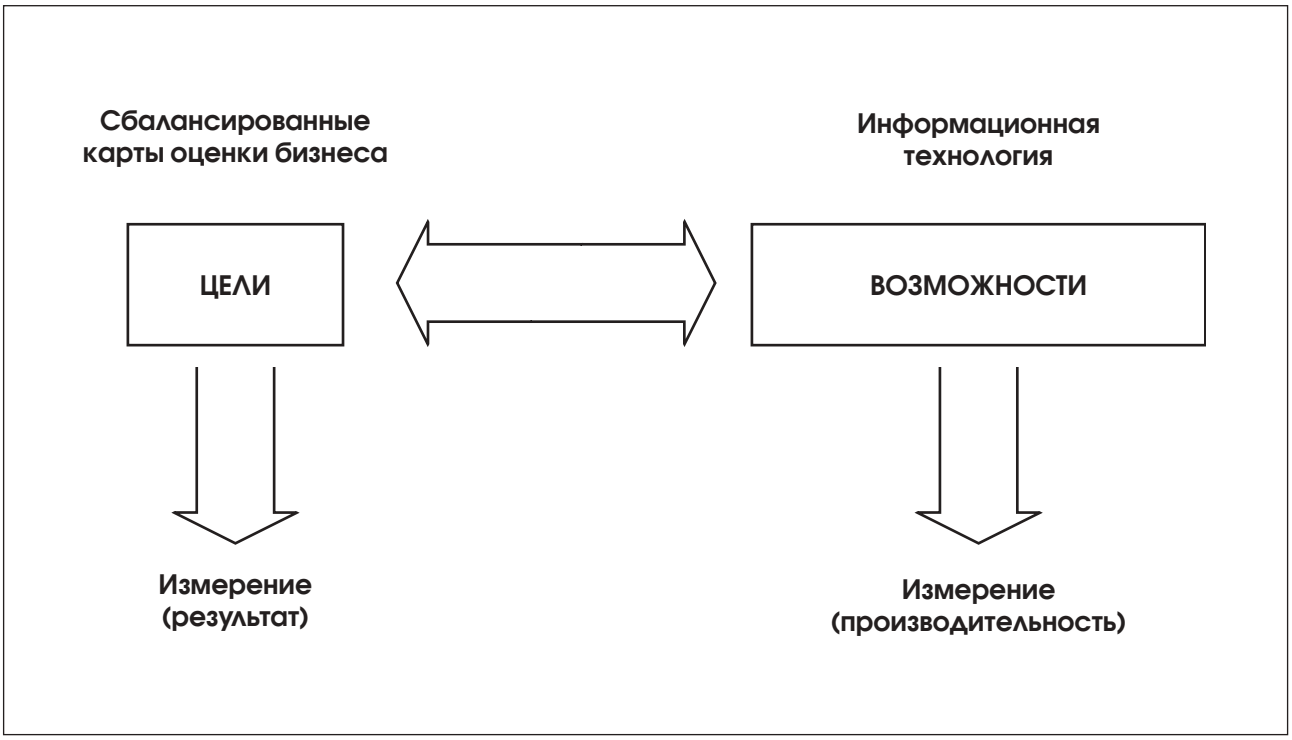


Рис. 5. Схема отношения бизнес целей и ИТ

ствие 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. 5).

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 явля-

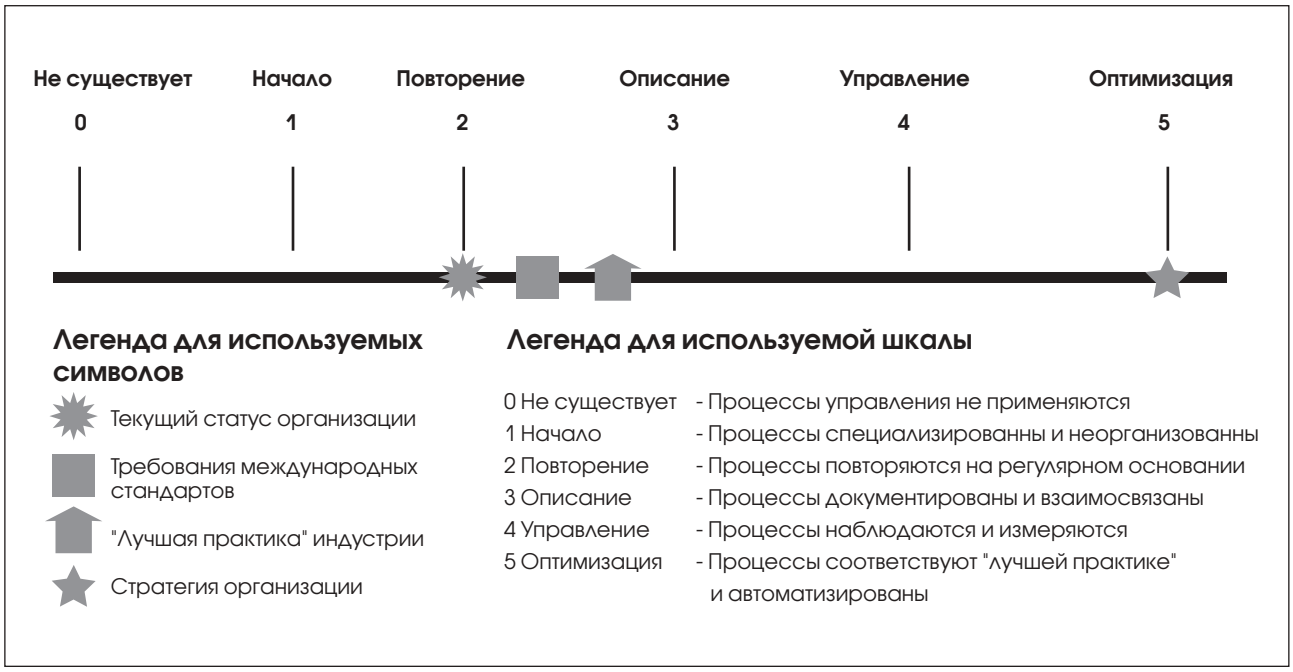


Рис. 6. Шкала моделей зрелости

ется 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.

Модели зрелости

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 (MM) — «модели зрелости». Соответствие уровням «модели зрелости» означает, что компания готова к плановой модернизации или обновлению. MM — 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. 6), 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.

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*.

Принципы аудита ИТ, стандарт CobiT

Принципы аудита CobiT — книга стандарта, которая в большей степени ориентирована на аудит ИТ-процессов, чем на аудит конкретных функций или приложений. CobiT состоит из высокоуровневых целей контроля (определенных для ИТ-процессов организации), которые охватывают все параметры информационных систем и применяемых информационных технологий, учитывают цикл жизни и специфические задачи, решаемые ИТ.

CobiT Advisor 3rd Edition (Audit)

Цель написания программного продукта «CobiT Advisor» — максимально облегчить проведение аудита ИТ. Основываясь на открытом стандарте CobiT, программа Advisor обновляется в соответствии с редакциями стандарта. На основании изменений и дополнений третьего издания стандарта CobiT в «CobiT Advisor» были внесены соответствующие изменения. Программный продукт был дополнен 16 новыми объектами контроля и новыми формами отчетов. «CobiT Advisor» представляет собой базу данных Foxpro, структурированную в соответствии с 34 процессами и 318 объектами контроля стандарта CobiT, которая позволяет хранить, обрабатывать и предоставлять информацию о результатах проведения аудита в форме отчетов в различных форматах (например, MS Word, Excel).

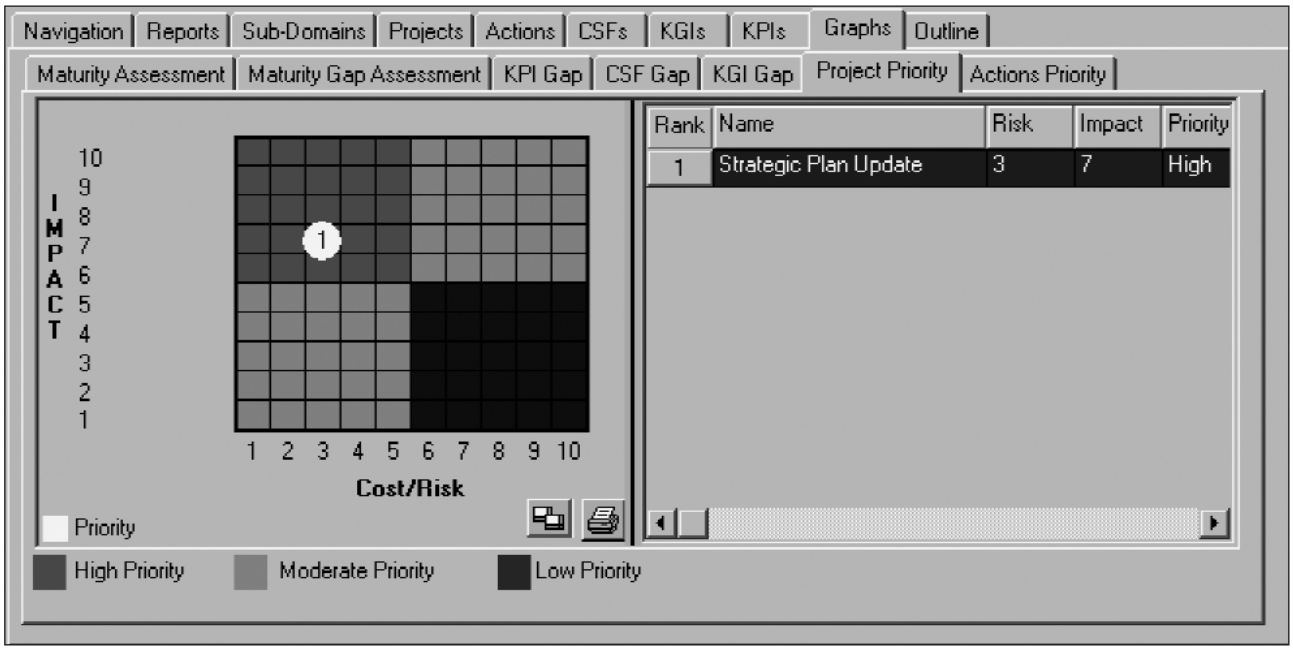


Рис. 7. Экран CobiT Advisor 3rd Edition

Одним из типовых отчетов являются модели зрелости, которые можно построить как для каждого процесса управления ИТ, так и для совокупной модели зрелости всех ИТ-сервисов организации (рис. 7).

Этика аудитора ИТ

Для обеспечения высокого качества оказания услуг, обеспечения профессионализма аудиторов ИТ и разрешения сложных этических ситуаций, возникающих в процессе аудита ИТ, ассоциация ISACA определила основные требования к аудитору ИТ. Они описаны в «Этическом кодексе аудитора».

Этический кодекс аудитора (Ассоциация ISACA)

1. Содействовать приведению информационных систем в соответствие с принятыми стандартами и руководствами;
2. Осуществлять свою деятельность в соответствии со стандартами в области аудита информационных систем, принятыми THE INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA);
3. Действовать в интересах работодателей, акционеров, клиентов и общества в старательной, лояльной и честной манере;
4. Сознательно не принимать участия в незаконной, либо недобросовестной деятельности;
5. Сохранять конфиденциальность информации, полученной при выполнении своих должностных обязанностей;
6. Не использовать конфиденциальную информацию для получения личной выгоды и не передавать ее третьим лицам без разрешения ее владельца;
7. Выполнять свои должностные обязанности, оставаясь независимым и объективным;
8. Избегать деятельности, которая ставит под угрозу независимость аудитора;
9. Поддерживать на должном уровне свою компетентность в областях знаний, связанных с проведением аудита информационных систем, принимать участие в профессиональных мероприятиях;
10. Проявлять добросовестность при получении и документировании фактографических материалов, на которых базируются выводы и рекомендации аудитора;
11. Информировать все заинтересованные стороны о результатах проведения аудита;
12. Способствовать повышению осведомленности руководства организаций, клиентов и общества в вопросах, связанных с проведением аудита информационных систем;
13. Соответствовать высоким этическим стандартам в профессиональной и личной деятельности;
14. Совершенствовать свои личные качества.

Структура принципов аудита CobiT

Для каждого ИТ-процесса, определенного CobiT, в *Принципах аудита* представлена следующая информация.

Секция высокого уровня принципов аудита CobiT отражает:

- Название бизнес-процесса;
- Требования бизнеса (Объекты контроля высокого уровня);
- Как осуществлять контроль;
- Что учитывать.

Для перехода на уровень детального аудита ИТ-процесса:

- Детальные объекты контроля;
- Как понять ИТ-процесс (кому задавать вопросы);
- Как оценить контроль ИТ-процесса;
- Как оценить соответствие этого контроля — управлению;
- Как доказать риск не выполнения целей управления.

На практике при проведении аудита для каждого ИТ-процесса ИТ-аудитору, как минимум необходимо выполнить следующую работу:

1. Определить высокоуровневый объект контроля;
2. Определить ИТ-процесс;
3. Проанализировать границы аудита;
4. Определить детальные объекты контроля;
5. Провести интервью с сотрудниками (ориентировочные названия должностей для каждого объекта контроля приведены в принципах управления);
6. Назначить задания на оценку средств контроля (Принято ли во внимание ...);
7. Оценить соответствие;
8. Проверить доказательства.

Уровень 1 Базовый уровень аудита ИТ	Структура CobiT Принципы аудита CobiT (стр. 22-24,29): • Требования процесса аудита • Контроль • Общие принципы аудита
Уровень 2 Процессы, описанные в принципах аудита	Принципы аудита CobiT (основная часть)
Уровень 3 Аудит дополнительных целей контроля	Специфические условия: • Специализированные отраслевые критерии • Промышленные стандарты • Требования производителей элементов инфраструктуры • Применение детальных методов контроля

Табл. 1. Применение книг стандарта CobiT при проведении аудита ИТ

Область охвата CobiT

В силу объективных причин у каждого из ИТ-специалистов разное образование, подготовка и опыт в сфере информационных технологий. Зачастую мы используем разные термины для описания одних и тех же событий, происходящих в информационной системе. На практике это приводит к недопониманию распоряжений руководства, выполнению излишней, ненужной работы, что, в свою очередь, мешает работе и сказывается на эффективности деятельности организации. Типичный пример, когда головной офис располагается в Москве, а офисы организации разбросаны по всей стране, и отчеты ИТ-служб с мест приходят в головной офис в виде, не поддающемся анализу. Руководители компаний пытаются решить эти и подобные проблемы доступными способами, самые популярные из которых — совещания по обмену опытом, дополнительное обучение и повышение квалификации сотрудников.

CobiT, в свою очередь, является своеобразной платформой для конструктивного диалога между всеми участниками процесса, формализуя через термины и определения общение между:

1. Топ-менеджерами;
2. Руководителями среднего звена (ИТ — директором, начальниками отделов);
3. Непосредственными исполнителями (инженерами, программистами и т.д.);
4. Внутренними и внешними аудиторами;
5. Подрядчиками работ.

CobiT предоставляет всем сотрудникам организации единую терминологию в сфере ИТ, гарантируя возможность общения на «одном языке», в частности, при открытии проектов, описании проблем и инцидентов и т.д. Облегчая управление и контроль, предоставляя компетентные однозначные ответы на вопросы, в том числе при внешних проверках.

Рассмотрим, каким образом стандарт CobiT может быть применен в повседневной деятельности организации? Рассмотрим организацию, которая ставит перед собой цель: «предоставлять на рынке собственные услуги при максимально высоком качестве». Для достижения этой цели организация формализовала свою деятельность в соответствии с рекомендациями набора стандартов ISO 9000, ISO/IEC TR 15504 SPICE и т.п. Допустим, что подавляющее большинство бизнес-процессов организации соответствует положениям ISO 9000, внедрение стандарта управляется и поддерживается высшим руководством организации. Как и у любого стандарта, предполагающего собственное внедрение, ISO 9000 запускает механизмы контроля и управления, но это механизмы контроля и управления бизнес-процессами организации. Вопросы же, связанные с ИТ, рассматриваются как неотъемлемая часть бизнес-процессов организации. Но при этом выделить ИТ-составляющую из общего результата достаточно проблематично, и, как следствие, на базе подобной информации затрудняется управление ИТ-составляющей.

Рассмотрим рисунок, иллюстрирующий процессы управления и аудита (Рис. 8).

Проведение аудита ИТ по стандарту CobiT представлено в левой части рисунка. Объекты контроля располагаются в соответствующих фазах бизнес-процессов, которые мо-

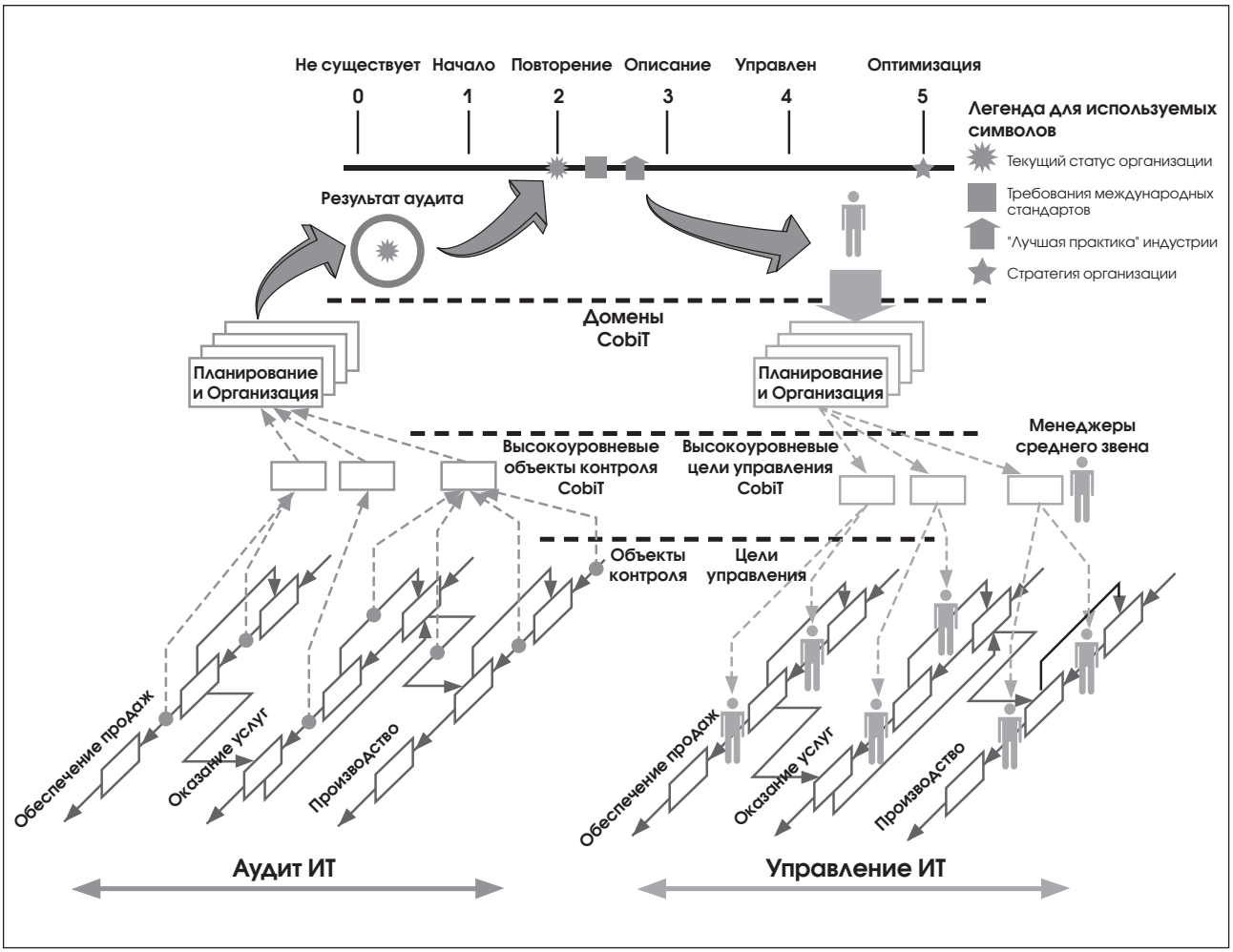


Рис. 8. Процессы управления и аудита

гут быть формализованы с соблюдением требований стандартов, предоставляя информацию с каждого объекта контроля на более высокий уровень. Рассматривая бизнес-процессы организации мы подразумеваем, что они могут быть созданы по стандартам качества или без них. Собираемая информация объединяется в высокоуровневые объекты контроля, которые затем сводятся в четыре домена CobiT. Оценка организации выводится на шкале модели зрелости организации, и лицу, принимающему решения, гарантируется возможность оценки текущего состояния ИТ в организации, сравнения с требованиями международных стандартов, а также с «лучшей» практикой и стратегией организации в той же отрасли.

Процессы управления схематично отражены в правой половине рисунка. По результатам проведенного обследования руководитель анализирует нужды и требования бизнес-процессов к ИТ, переходя тем самым к управлению. При этом необходимо принимать во внимание тот факт, что невозможно управлять организацией в соответствии с положениями стандарта CobiT (при этом не проводя аудит в соответствии с CobiT), который позволяет получить в достаточном объеме необходимую и достоверную информацию для принятия решений и наоборот. Таким образом, оба эти процесса должны осуществляться в соответствии с рекомендациями CobiT.

Для надлежащего управления ИТ по CobiT требуется информация, представляемая в соответствии с рекомендациями стандарта, а хотя аудит по CobiT проверяет информационные технологии организации на соответствие рекомендациям CobiT, наиболее существенную роль играет при этом интерпретация результатов. Таким образом, выпадение одного из звеньев из этой цепочки снижает уровень достоверности полученной информации и эффективности ее дальнейшего использования.

Взаимосвязь CobiT и других требований и стандартов

Открытый стандарт CobiT имеет свою нишу в общем комплексе стандартов, методик и руководств. Прежде всего, это стандарт управления и аудита ИТ. На что следует резонный вопрос, но, например, ITIL тоже содержит рекомендации по управлению ИТ-услугами, как они пересекаются? ITIL — библиотека лучшего практического опыта в части предоставления ИТ-услуг, а CobiT специализируется и на управлении и на аудите ИТ. Процессы ITIL, как и любые другие процессы, могут управляться и контролироваться стандартом CobiT.

Повторюсь, что для управления предназначены цели управления, изложенные в *Принципах управления*, а для аудита — объекты контроля, изложенные в *Принципах аудита*. На рисунке это разделение представлено схематично (рис. 9).

Как следует из рисунка, CobiT предоставляет топ-менеджерам возможность донести цели и задачи бизнеса до руководителей ИТ-служб, преобразовав стратегические и тактиче-

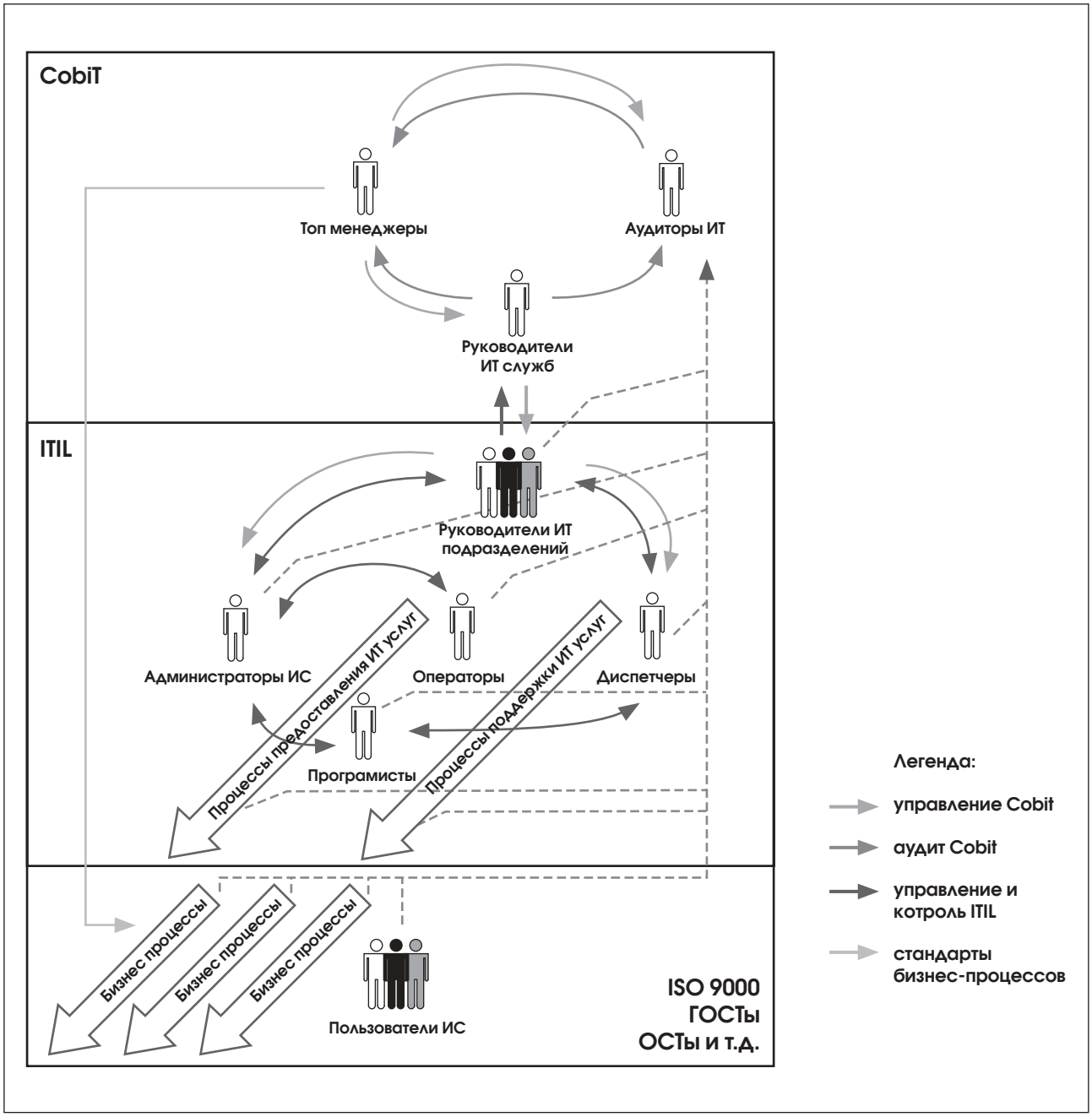


Рис. 9. Разделение объектов управления и аудита

ские планы организации в четкие и понятные планы развития ИТ. Руководители ИТ-служб, в свою очередь, управляют руководителями подразделений на основе полученных указаний в соответствии с CobiT. Методология ITIL применяется для оптимизации процесса обслуживания информационных систем с точки зрения управления. Если процессы предоставления и поддержки ИТ услуг (ITIL) в организации не внедрены, то Cobit предоставляет механизмы управления и на этом уровне. При этом CobiT можно применить в части управления эксплуатацией информационной системой, но только в качестве инструмента общего управления и контроля. Здесь необходимо учитывать, что CobiT не предоставляет инструментов для управления или аудита аппаратно-программного обеспечения конкретных фирм производителей. Так, например, аудит программного обеспечения Microsoft должен выполняться в соответствии с методиками, разработанными Microsoft, и на соответствие требованиям Microsoft, но результаты подобной проверки могут и должны быть использованы в процессах CobiT. Так очень схематично можно определить место и роль CobiT в части управления ИТ.

Итак, ИТ-аудиторы собирают, анализируют информацию и предоставляют отчеты и заключения руководителям организации в соответствии с руководством аудитора CobiT (объекты контроля, «размещенные» в соответствии с рекомендациями CobiT). Основываясь на аудиторских оценках и заключениях о степени достижения целей управления, руководители организации обоснованно, с точки зрения соответствия ИТ целям и задачам бизнеса, осуществляют управление процессами организации для реализации ее бизнес-целей.

Практические рекомендации

Как уже говорилось выше, главной связующей нитью между аудитом и управлением являются полученные результаты аудита, на основе которых в дальнейшем создается система управления. Результаты должны оформляться в виде отчета, минимальный перечень разделов которого приведен ниже:

1. Общий раздел.
2. Описание текущей ситуации.
3. Выводы и заключения.
4. Рекомендации.
5. Приложения, в которые включаются документы, результаты интервью и другая фактическая информация, на которой базируются заключения и рекомендации.

Содержание отчетов может варьироваться в зависимости от уровней предоставления информации:

1. **«Резюме для руководителей»** — резюме по результатам аудита объемом в 1-3 страницы, содержащих краткую оценку текущей ситуации, основные рекомендации с указанием ожидаемого эффекта, сопутствующие риски и указание ориентировочной стоимости. Документ предоставляется высшему руководству на уровне генерального директора, финансового директора, исполнительного директора.
2. **«Общий»** — полный отчет, созданный по результатам проведенного ИТ-аудита. Должен включать, как минимум, следующие разделы: описание текущей ситуации, выводы и заключения, рекомендации (детальные). Документ предоставляется менеджерам среднего звена.

В западной практике результатом аудита считается заключение аудиторской организации, на основании которого консультанты из этой же или другой фирмы, подготавливают рекомендации, направленные на повышение таких показателей организации, как эффективность, производительность, экономичность, качество и т.п. На российском рынке ИТ-консалтинга Заказчик в большинстве случаев требует от подрядчика (в основном от аудиторской компании) не только заключения и рекомендаций, но и их реализации, хотя бы до стадии проведения тендеров на поставку оборудования или услуг.

Преимущества проведения регулярного аудита

На практике в большинстве организаций необходимый уровень управления обеспечивается внутренней иерархией: вершину дерева занимает лицо, принимающее решение, например, генеральный директор, консультант по ИТ, директор департамента ИТ. Управление осуществляется через менеджеров среднего звена (руководителей департаментов, отделов, рабочих групп, менеджеров проектов). Контроль выполнения руководящих указаний обеспечивается формальными отчетами о проделанной работе, при этом полнота и объективность отчетов остается на совести исполнителей работ. Одним из решений задач управления и контроля в сфере информационных технологий организации является создание собственного подразделения внутреннего аудита ИТ.

Основным преимуществом регулярного проведения аудита является накопление знаний организации, создание собственной базы знаний, которая позволит быстро и достоверно ответить на большинство вопросов, возникающих в организации.

Внутренний аудит предоставляет отчеты и информацию по запросу в любое время, а внешний (сторонние аудиторы) — лишь после заключения и соблюдения договорных обязательств. Построение и поддержка актуальности базы знаний об ИТ-организации позволит обеспечить прозрачность ИТ-служб, организовать эффективное взаимодействие служб ИТ, эффективно управлять ИТ.

Таким образом, делая выбор, базирующийся на возможностях и целях организации, придется выбирать между подрядом внешней команды с расчетом на долгосрочное сотрудничество или лишь для проверки результатов «первичного» аудита, который в дальнейшем попадает в сферу компетенции внутренней аудиторской службы. То есть сторонние аудиторы, проводя первичный аудит, позволяют руководителям, в том числе и с точки зрения временного задела, сконцентрировать усилия на создании высокопрофессиональной службы внутренних аудиторов к моменту сдачи результатов проверки.

Как мы уже выяснили, «первичный» аудит отличается от последующих относительной сложностью и большим объемом собираемой и анализируемой информации. Руководитель организации, заказавший аудит ИТ у внешней аудиторской компании, должен понимать, что через полгода-год (в зависимости от динамики развития) ситуация в организации изменится, результаты аудита потеряют свою актуальность.

«Первичный» аудит — термин не общепринятый, но все же, это состояние, когда информация об ИТ-организации собирается впервые.

Если в этот момент не провести повторный аудит для сравнения с предыдущими результатами, то деньги, вложенные в «первый» аудит, можно считать потерянными и придется проводить «первичный» аудит заново.

Идеальная ситуация, когда аудит и управление выполняются по CobiT, предоставляя лицу, принимающему решение, полнофункциональный инструмент управления и контроля над ИТ организации, но на практике мы сталкиваемся с отсутствием формального управления.

В этом случае требуется дополнительная предварительная работа, направленная на описание производственных процессов организации.

Причины постановки управления и проведения аудита ИТ

Аудит ИТ проводят для того, чтобы оперативно **получать** систематизированную и достоверную **информацию для оценки ИТ, принятия решения, управления ИТ.**

Результаты аудита ИТ позволяют:

1. **Оценить соответствие ИТ требованиям бизнеса**
   - Выявить недостатки и упущения;
   - Обосновать инвестиции в ИТ.
2. **Прогнозировать развитие ситуации**
   - Эффективно планировать развитие ИТ-организации;
   - Понимать выгоды и риск при внесении изменений в информационную систему;
   - Прогнозировать возникновение проблемных ситуаций (проблем и инцидентов).
3. **Принимать решения**
   - Обоснованно решать проблемы безопасности и контроля;
   - Обоснованно приобретать или модернизировать аппаратно-программные средства;
   - О приобретении услуг (outsourcing);
   - Планировать повышение квалификации сотрудников ИТ-подразделений.
4. **Контролировать исполнение решений**
   - Управлять ИТ составляющей проектов (контролировать время и стоимость их реализации, оценивать полноту достижения целей);
   - Контролировать стоимость владения ИС.

Причины применения стандарта CobiT для управления и аудита ИТ

После проведения ИТ-аудита с использованием принципов аудита, изложенных в CobiT, организация получит возможность:

1. Оценить степень соответствия ИТ-организации требованиям бизнеса.
2. Определить приоритеты основных ИТ-процессов.
3. Выявить критически важные элементы ИТ.
4. Выявить и оценить факторы риска.
5. Определить степень адекватности мер, принимаемых для управления рисками.
6. Оценить степень защищенности компании от чрезвычайных происшествий и их последствий.
7. Реализовать рекомендации по обеспечению бесперебойности функционирования ИТ.
8. Создать план работ по устранению недостатков и разработать способы их устранения.

Кроме того, управление и аудит в соответствии со стандартом CobiT предоставляет организации следующие дополнительные преимущества:

1. Возможность получения результата в сравнительно короткие сроки.
2. Гарантия того, что при проведении аудита ничто не будет забыто: стандарт охватывает все уровни ИТ.
3. После проведения «первичного» аудита производится наполнение информационной базы, что делает процессы проведения последующих проверок проще, легче и, как следствие, дешевле.
4. CobiT как инструмент управления остается и внедряется в организации, автоматически переводя ее на уровень управления, сопоставимый, как минимум, со 2 уровнем модели зрелости CMM, несмотря на то, что достижение уровней зрелости не является прямой целью аудита — это специфические задачи бизнес-консалтинга.

Предложение услуг по ИТ аудиту на Российском рынке

На Российском рынке в настоящее время, в части предложения услуг по проведению ИТ-аудита, очень условно можно выделить следующие виды:

- **Обследование ИТ**, частный случай это обычная инвентаризация — сбор информации, которая будет использоваться для проведения последующих работ, например, проектных работ, когда требуется грамотно собрать достоверную информацию о текущем состоянии ИТ. Основную роль здесь играет сбор и структуризация информации, анализ и оценка не производится.
- **Экспертная оценка ИТ** — оценка ИТ-проектов (проектных решений), оценка правильности (обоснованности) инвестиций в ИТ, сколько стоит ИТ-составляющая организации, не только балансовая стоимость компьютеров и программ, но и долгосрочность примененных проектных решений, оценка текущих ИТ-проектов, возможность перепрофилирования существующей ИТ-инфраструктуры под решение качественно других задач, организация эксплуатации ИТ, подготовка пользователей. Мы не говорим об возврате инвестиций, это тема отдельного исследования, мы говорим об оценки адекватности финансирования проектных решений, инвестиций в закупку оборудования и ИТ-услуг. Большинство современных компаний строят свой бизнес, взаимодействуют с клиентами и партнерами с широким применением информационных технологий. Однако существующие в настоящее время методики оценки предприятий сведены к экспертным заключениям о денежных потоках, материальных активах, финансовых показателях текущей деятельности и т.д., практически не учитывая совокупной стоимости и значимости для бизнеса информационных ресурсов предприятия.
- **Технический аудит ИТ** — сбор, анализ информации и выдача рекомендаций по улучшению работы отдельного элемента ИТ-инфраструктуры. Характерные особенности — малый масштаб работы («железка» с ее входами-выходами) и узкая прикладная специализация исследования, можно сказать что это «штучная» работа, для каждого конкретного случая.
- **Аудит ИТ бизнес-процесса** – Аудит информационных технологий, поддерживающих определенный (выделенный или заданный) бизнес-процесс организации на соответствие заданным (или разработанным) критериям оценки. Для проведения подобного аудита необходимо определить ответственного за процесс, пользователей и участников, выявить применяемое оборудование и программы, обслуживающий персонал, проектные и регламентирующие документы. На базе собранной информации построить модель, с указанием мест взаимодействия (стыка) с другими бизнес-процессами.
- **Аудит критерия ИТ** — сбор, анализ информации и выдача рекомендаций по какому-то выбранному критерию ИТ: безопасность, производительность, надежность, доступность и т.д. При проведении аудита по определенному критерию оценки мы говорим не только об отдельном элементе ИТ-инфраструктуры, но и обо всей совокупности программных, аппаратных средств, процессов их сопровождения и обслуживания во всей проверяемой организации.
- **Комплексный аудит ИТ.** Руководство должно знать и иметь возможность оценить все, что происходило и происходит в ИТ-организации, сравнить адекватность ИТ-потребностям бизнеса. Иначе говоря, прогнозировать развитие организации и соизмерять его с текущим состоянием и перспективами развития ИТ. В результате получается сложная многомерная матрица взаимосвязей бизнес-процессов, их требований, информационных и смежных технологий, совокупности программно-аппаратных средств их возможностей/ограничений и многого другого должна быть представлена в виде простого и понятного образа, при этом сохранив достоверность информации. Информации об успешной реализации таких проектов в России очень мало, потому что, прежде всего, это требует объединения ресурсов различных компаний и организации единой коллективной работы.

Приведенная классификация, является условной, автор будет благодарен за любые отзывы о ней как ИТ-специалистов, маркетологов, так и других заинтересованных лиц.

Заключение

Перефразируя утверждение, что «у каждой бумаги должны быть ноги», можно сказать, что у каждого стандарта должна быть голова. CobiT не является исключением, именно его переосмысление и адаптация под нужды каждого конкретного Заказчика, будь то ИТ-руководитель, внешний или внутренний аудитор, либо консультант — это большая ежедневная работа.

Термины и определения

Аудит — Что такое аудит? Что под этим термином понимается? Определений как таковых много, на мой взгляд, наиболее лаконичным и верным по сути является трактовка Комитета Американской бухгалтерской ассоциации по основным концепциям учета: «Аудит — это системный процесс получения и оценки объективных данных об экономических действиях и событиях, устанавливающий уровень их соответствия определенному критерию и предоставляющий результаты заинтересованным пользователям...».

В данном случае для осознания, что есть такое аудит ИТ, необходимо лишь изменить обозначенную в приведенном выше определении область применения, экономическую на интересующую нас сферу информационных технологий. Таким образом, **Аудит ИТ** — системный процесс получения и оценки объективных данных о текущем состоянии информационной системы, действиях и событиях, происходящих в ней, устанавливающий уровень их соответствия определенным критериям и предоставляющий результаты Заказчику.

Стандарт аудита — нормативно-технический документ (или эталон, модель, которая является отправной точкой), устанавливающий комплекс требований и правил к объекту аудита, квалификации исполнителей, организации аудита, методическим приемам анализа документации и представлению аудиторского заключения в предметной области и т.д.

Методика аудита — совокупность теоретических и практических способов проведения аудита, разработанные аудитором на базе стандартизированных правил и норм проведения аудита в предметной области, в определенной степени, на основе личного профессионального опыта.

Информационно-коммуникационные технологии (определение Информационного общества www.iis.ru) — совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей.

Каждое предприятие осуществляет определенную деятельность, направленную на достижение своих стратегических целей и удовлетворение потребностей. Любую деятельность можно разбить на функционально законченные процессы (для коммерческих предприятий — бизнес процессы). В качестве ключевых обычно выделяют: производство, сбыт, продвижение продукции, управление и другие процессы, типичные для большинства предприятий. Роль информационных технологий (ИТ) заключается в поддержке деятельности предприятия. ИТ должны обеспечить выработку правильного управленческого решения в каждой конкретной ситуации, т. е. в нужное время, в нужном месте и в нужном объеме дать достоверную информацию, необходимую для принятия управленческого решения.

Смежные технологии — смежные с ИТ сферы деятельности: инженерные системы (например, концепция интеллектуального здания, включающая в себя гарантированное электропитание, кондиционирование, водоснабжение и т.д.). *Технологии, не относящиеся к информации, но являющиеся критически важными для нее это пример, знакомый страховщикам, — выплата страховки за страховой случай, связанный с пожаром или затоплением серверной.* На данный момент практически все компании, предлагающие комплексные ИТ решения обладают наряду с лицензиями на осуществление оценочной и аудиторской деятельности еще и лицензиями на строительство и проектирование зданий и сооружений. Что само иллюстрирует неразрывную связь между указанными технологиями.

Информационные системы (определение Информационного общества www.iis.ru) — орга-

низационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Глоссарий

Одним из недостатков на российском ИТ рынке является отсутствие единой терминологической базы, чтобы точно обозначить термины, взятые мной из первоисточников, привожу краткий глоссарий примененный к ключевым терминам данной статьи.

IT Governance Institute — Институт Управления ИТ
Information and related Technology — Информационные и смежные Технологии
high-level approach — высокоуровневый подход
Maturity Models — Модели Зрелости
Critical Success Factors (CSFs) — Критические Факторы Успеха (КФУ)
Key Goal Indicators (KGIs) — Ключевые Индикаторы Цели (КИЦ)
Key Performance Indicators (KPIs) — Ключевые Индикаторы Результата (КИР)
Networking — сеть организации (ЛВС)
management of IT related risks — Управление сопутствующими рисками в ИТ
enterprise governance — управление предприятием
IT governance — управление ИТ
Dashboards — инструментальная панель
Scorecards — карты оценок
Balanced Business Scorecard — Сбалансированные карты оценки бизнеса
Measures — единицы измерения
Benchmarking — эталонное тестирование
Scale for comparison — шкала сравнения
Effectiveness — Эффективность
Efficiency — Продуктивность
Confidentiality — Конфиденциальность
Integrity — Целостность
Availability — Пригодность
Compliance — Согласованность
Reliability — Надежность
Cost-efficiency — рентабельность

Книги CobiT

Executive Summary — Резюме для руководителей
CobiT Framework — Структура CobiT
Control Objectives — Объекты Контроля
Management guidelines — Принципы управления
Audit guidelines — Принципы аудита

Источники информации и полезные ссылки

«The Balanced Business Scorecard — Measurements that Drive Performance,» Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992
«Capability Maturity ModelSM for Software,» Version 1.1. Technical Report CMU/SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993
http://www.isaca.org
http://www.pinkelephant.org
http://www.isaca.ru
http://itsm.itpark.ru/
http://www.methodware.com
http://krilov.lib.ru

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания Джет Инфо Паблишер
Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Технический редактор: Овчинникова Г.Ю. *(galya@jet.msk.su)*
Россия, 127006, Москва, Краснопролетарская, 6
тел. (095) 972 11 82, 972 13 32
факс (095) 972 07 91
email: JetInfo@jet.msk.su http://www.jetinfo.ru
Подписной индекс по каталогу Роспечати 32555