Презентация на тему «Принципы аудита состояния информационной инфраструктуры»

СТАРОВЕРОВА О.В.

Основные понятия и концепция аудита информационной инфраструктуры

В настоящее время информационные технологии являются одним из основных инструментов обеспечения адаптивности и конкурентоспособности современных хозяйствующих
субъектов. По мере изменения требований внешнего окружения этих субъектов меняются требования, предъявляемые к программным продуктам и ИТ-сервисам, что приводит к добавлению в их информационную инфраструктуру все новых и новых программно-аппаратных платформ. При этом все возрастающая их сложность и разнородность оказывают влияние на управляемость всей информационной инфраструктуры, стабильность и эффективность ее работы.

Под **информационной инфраструктурой** в данном контексте следует понимать отлаженную систему (подсистему), выполняющую функции обслуживания, документирования, учета, контроля и анализа всех процессов, происходящих с информационными потоками хозяйствующего субъекта. Иными словами, «**инфраструктура** – это технология и устройства (например, аппаратное обеспечение, операционные системы, системы управления базами данных, сетевое обору-дование, мультимедиа, а также та среда, в которой все это находится и поддерживается), которые обеспечивают работу приложений».

В свою очередь, под **информационной технологией** понимают «систему правил, определяющих способы сбора, накопления, регистрации, передачи, обработки, хранения, по- иска, модификации, анализа, защиты, выдачи необходимой информации всем заинтересованным подразделениям или отдельным пользователям»

Основные понятия и концепция аудита информационной инфраструктуры

Сам подход к проведению аудита информационных инфраструктур с течением времени упорядочился и стандартизировался. Крупные аудиторские компании образовали ассоциации профессионалов в указанной предметной области, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ.

Однако это, как правило, закрытые для общественности стандарты. Поэтому для удовлетворения все нарастающей потребности в координации действий аудиторов и централизации хранения знаний управления информационными системами в 1967 году не- большая группа профессионалов основала Ассоциацию аудита и контроля информационных систем (Information Systems Audit and Control Association – ISACA).

Сегодня ISACA является признанным мировым лидером в области управления, контроля и аудита информационных технологий и информационной безопасности, а также управления информационными рисками. В настоящее время членами ISACA являются более 86000 профессионалов, работающих более чем в 160 государствах, которые являются специалистами в самых различных областях знаний, связанных с управлением, аудитом и эксплуатацией ИТ. Основная декларируемая цель Ассоциации – исследование, разработка, публикация и продвижение стандартизированного набора документов по управлению информационными технологиями для ежедневного использования администраторами и аудиторами ИТ.

Этический кодекс аудитора информационных систем

Наряду со стандартами ISACA разработала **Этический кодекс аудитора информационных систем** (Code of Professional Ethics), который обязателен к соблюдению всеми аудиторами, практикующими в рассматриваемой предметной области.

Основные принципы Кодекса гласят:

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 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 фотографических 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.

Этический кодекс аудитора информационных систем

Указанные требования призваны обеспечить высокое качество оказания аудиторских услуг, профессионализм самих аудиторов, а также разрешать сложные этические ситуации, возникающие в процессе аудита информационных технологий.

Стандарты аудита и управления, разработанные Ассоциацией, вобрали в себя опыт профессионалов всего мира. Исследования, проводимые в рамках Ассоциации, соответствуют все возрастающим требованиям ее членов и потребностям реальной действительности. В настоящее время, наряду с исследовательской и регламентационной работой, Ассоциация присваивает высококвалифицированным специалистам международные сертификаты, признаваемые во всем мире:

- сертифицированный аудитор информационных систем (Certified Information Systems Auditor – CISA);
- сертифицированный менеджер информационной безопасности (Certified Information Security Manager – CISM);
- сертифицированный специалист в области корпоративного управления ИТ (Certified in the Governance of Enterprise IT – CGEIT).

За три десятилетия своего существования ISACA разработала и постоянно обновляет такие общепризнанные в мире международные стандарты, как «Контрольные объекты для информационных и смежных технологий» (Control Objectives for Information and Related Technology – Cobit) и «Управление инвестициями в ИТ» (Val IT). Структура и содержание указанных стандартов позволяют обеспечить методологической поддержкой все уровни руководства системы управления любым хозяйствующим субъектом.

Этический кодекс аудитора информационных систем

Указанные требования призваны обеспечить высокое качество оказания аудиторских услуг, профессионализм самих аудиторов, а также разрешать сложные этические ситуации, возникающие в процессе аудита информационных технологий.

Стандарты аудита и управления, разработанные Ассоциацией, вобрали в себя опыт профессионалов всего мира. Исследования, проводимые в рамках Ассоциации, соответствуют все возрастающим требованиям ее членов и потребностям реальной действительности. В настоящее время, наряду с исследовательской и регламентационной работой, Ассоциация присваивает высококвалифицированным специалистам международные сертификаты, признаваемые во всем мире:

- сертифицированный аудитор информационных систем (Certified Information Systems Auditor – CISA);
- сертифицированный менеджер информационной безопасности (Certified Information Security Manager – CISM);
- сертифицированный специалист в области корпоративного управления ИТ (Certified in the Governance of Enterprise IT – CGEIT).

За три десятилетия своего существования ISACA разработала и постоянно обновляет такие общепризнанные в мире международные стандарты, как «Контрольные объекты для информационных и смежных технологий» (Control Objectives for Information and Related Technology – Cobit) и «Управление инвестициями в ИТ» (Val IT). Структура и содержание указанных стандартов позволяют обеспечить методологической поддержкой все уровни руководства системы управления любым хозяйствующим субъектом.

Контрольные объекты для информационных и смежных технологий

Стандарт Cobit в настоящее время является синтезом четырех десятков международных стандартов в области аудита, контроля, управления информационными технологиями и информационной безопасности. Его основной стратегической задачей является ликвидация разрыва между руководящим звеном системы управления хозяйствующими субъектами с их видением целевой направленности деятельности этих субъектов и ИТ департаментами, осуществляющими поддержку важнейшей для любого функционирующего хозяйствующего субъекта информационной инфраструктуры, которая должна быть направлена на достижение этих целей.

Стандарт Cobit определяет и регламентирует обязательные требования, предъявляемые к аудиту и к отчетным формам, оформляемым по его результатам. Он предоставляет:

- аудиторам: минимально приемлемый уровень исполнения работ в соответствии с профессиональными требованиями Кодекса профессиональной этики;
- сертифицированным аудиторам информационных систем: обязательные требования, предъявляемые к их работе;
- менеджерам и иным заинтересованным лицам: представления о требуемом уровне профессиональной работы лучших практиков в области ИТ.

Указанный стандарт раскрывает лучший практический опыт на уровне доменов (групп ИТ-процессов) и отдельных процессов, а также регламентирует действия в виде управляемой и логичной структуры. При этом лучший практический опыт основан на консенсусе экспертов. Он (опыт) в большей степени ориентирован на контроль, нежели на исполнение. Раскрытые в Стандарте нормы позволяют оптимизировать инвестиции в информационные технологии, обеспечить уверенность в уровне предоставляемых сервисов и выработать показатели, на которые можно ориентироваться в случае неблагоприятного развития ситуации.

Контрольные объекты для информационных и смежных технологий

В сфере информационных технологий предоставление сервисов, соответствующих требованиям деятельности хозяйствующего субъекта, предполагает наличие надлежащей системы и методологии внутреннего контроля. Система контроля, основанная на Cobit, отвечает этим требованиям, поскольку:
связана с требованиями деятельности хозяйствующих субъектов;

- организует виды ИТ-деятельности в виде понятной процессной модели;
- определяет основные ресурсы ИТ, на которые должны осуществляться воздействия;
- определяет цели контроля.

Ориентация стандарта Cobit на деятельность хозяйствующих субъектов состоит во взаимосвязи целей этой деятельности и информационных технологий, выявлении показателей и моделей зрелости для оценки достижений, определении степени ответственности владельцев бизнес и ИТ- процессов. Иными словами, в основу стандарта Cobit положено основополагающее утверждение, что для обеспечения любого хозяйствующего субъекта (его системы управления) информацией, необходимой для достижения определенных бизнес целей, следует управлять ИТ-ресурсами с помощью естественным образом сгруппированных ИТ-процессов.

Первая версия стандарта Cobit, выпущенная в 1996 году, включала в себя «Концептуальное ядро» (Cobit Framework), определяющее набор основополагающих принципов и понятий в области управления информационными технологиями, описание Объектов контроля (Control Objectives) и «Руководство по аудиту» (Audit Guidelines).
Вторая версия была опубликована в 1998 году. В нее вошли переработанная версия «Детальных объектов контроля» (Detailed Control Objectives) и «Набор инструментов внедрения» (Implementation Tool Set).
В третью версию стандарта вошло «Руководство по управлению» (Management Guidelines), в основу которого заложено понятие «Система управления ИТ» (IT Governance). Таким образом, в состав третьей редакции Стандарта Cobit вошло несколько книг, ориентированных на различных потребителей.

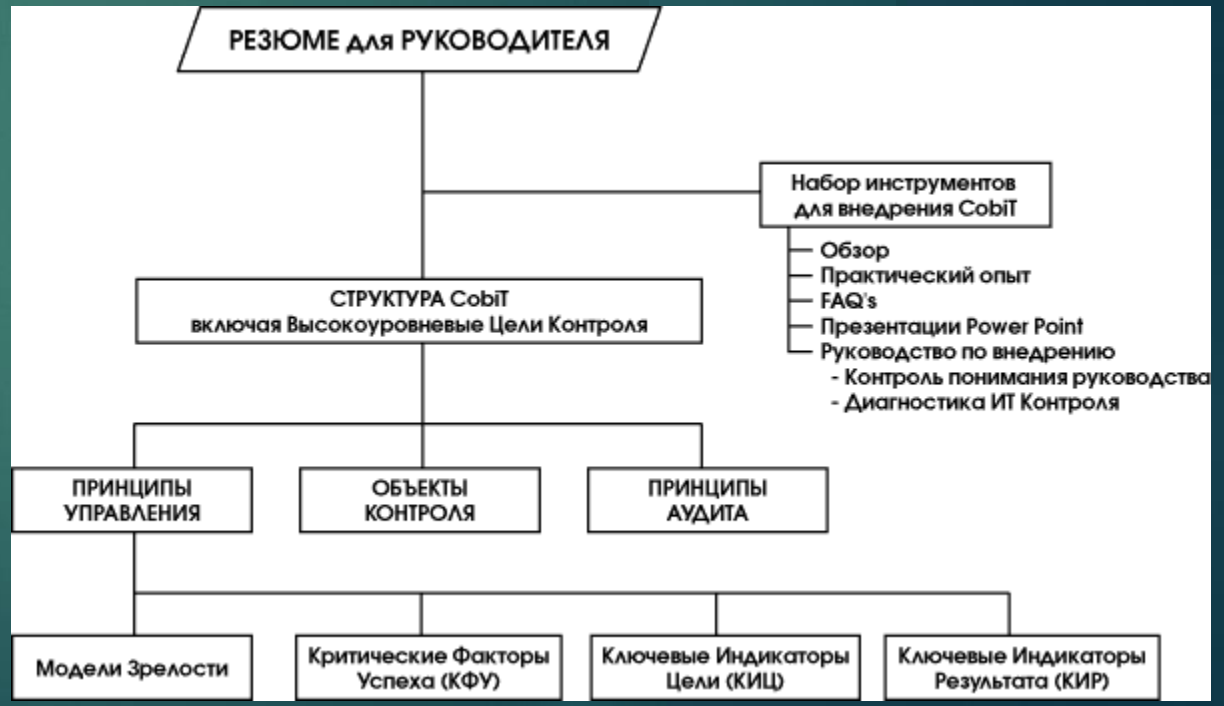
Состав книг стандарта Cobit

Таким образом, в состав третьей редакции Стандарта Cobit вошло несколько книг, ориентированных на различных потребителей.
При этом «Резюме для руководства» служит введением в остальные разделы Стандарта и ориентировано на высшее звено системы управления хозяйствующим субъектом для принятия ими решения о применении Стандарта Cobit в их субъекте. Оно определяет Миссию Cobit и понятие Системы управления ИТ.
В свою очередь, Концептуальное ядро (или Структура Cobit) содержит развернутое описание структуры стандарта, высокоуровневых целей контроля и пояснения к ним. Основная концепция Cobit предполагает формирование механизмов управления в информационных технологиях исходя из того, какая информация необходима для поддержания целей деятельности хозяйствующего субъекта и удовлетворения требований этой деятельности.
Информация в данном контексте рассматривается как результат использования ИТ- ресурсов, управление которыми осуществляется в рамках ИТ- процессов.

Концептуальное ядро Cobit сгруппировано в четыре домена (группы ИТ-процессов):

- планирование и организация (planning and organization) – определяющие направления относительно внедрения решений и обеспечения сервисов;
- приобретение и внедрение (acquisition and implementation) – обеспечивающие внедрение решений и оказание на их основе сервисов;
- эксплуатация и сопровождение (delivery and support) – представляющие сами решения и делающие их применимыми для конечных пользователей;
- мониторинг (monitoring) – выполняют надзор за всеми процессами для того, чтобы убедиться в продвижении в верном направлении.

Указанные домены объединяют в себе 34 высокоуровневых задачи (объекта) управления (одна задача для каждого ИТ-процесса).



Состав книг стандарта Cobit

Книга «Детальные объекты контроля» раскрывает детальное описание объектов (задач) контроля для каждого из 34 ИТ-процессов. Всего насчитывается 318 объектов. «Руководство по управлению» позволяет руководству хозяйствующего субъекта реализовать наиболее эффективные стратегии управления информационными технологиями, установить контроль над использованием информационных ресурсов и соответствующими процессами, осуществлять мониторинг, давать сравнительную оценку достижения целевых установок хозяйствующего субъекта и оценивать эффективность в рамках каждого ИТ-процесса. «Набор инструментов внедрения» содержит разъяснения ключевых концептуальных положений стандарта Cobit, а также алгоритм процесса их внедрения в деятельность любого хозяйствующего субъекта.

Книга включает в себя следующие основополагающие компоненты:

- обзорная часть (Executive Overview);
- руководство по внедрению, включая практический опыт и презентации (Case Studies, Power Point Presentations);
- инструментарий, помогающий анализировать структуру управления ИТ хозяйствующего субъекта: Диагностика осведомленности руководства субъекта (Management Awareness Diagnostic) и Диагностика ИТ-управления (IT Control Diagnostic);
- часто задаваемые вопросы и ответы на них (FAQs).

Процесс внедрения Стандарта Cobit в деятельность хозяйствующего субъекта состоит из следующих основных этапов:

1) определение цели деятельности на основе Концептуального ядра стандарта;
2) выбор ИТ-процессов и механизмов управления на основе высокоуровневых и детальных объектов управления;
3) разработка и согласование программы внедрения с бизнес-планом;
4) оценка существующих процедур и результатов внедрения механизмов управления на основе «Руководства по аудиту»;
5) оценка текущего статуса хозяйствующего субъекта, идентификация критических действий, ведущих к успеху, и измерение эффективности достижения целевых установок деятельности хозяйствующего субъекта на основе «Руководства по управлению».

И наконец, «Руководство по аудиту» представляет собой книгу, ориентированную на аудит ИТ-процессов.

Принципы аудита информационных технологий

Аудит позволяет оперативно получать систематизированную и достоверную информацию не только для оценки ИТ, но и для принятия адекватных решений по управлению ими. На российском рынке в настоящее время можно выделить шесть видов услуг по аудиту информационной инфраструктуры:

- обследование информационных технологий, применяемых хозяйствующим субъектом;
- экспертная оценка адекватности финансирования проектных решений и/или инвестиций в закупку оборудования и ИТ-сервисов;
- технический аудит информационных технологий;
- аудит ИТ-процессов;
- аудит критерия информационных технологий;
- комплексный аудит информационной инфраструктуры.

Обследование информационных технологий предполагает всего лишь сбор информации (инвентаризация) для проведения последующих работ по внедрению нового информационного элемента инфраструктуры. При этом анализ и оценка не производятся. В свою очередь, экспертная оценка предполагает осуществление следующих видов оценки:

- оценка ИТ-проектов или проектных решений;
- оценка обоснованности инвестиций в информационные технологии;
- оценка стоимости ИТ-составляющей хозяйствующего субъекта;
- оценка текущих ИТ-проектов;
- оценка возможности перепрофилирования информационной инфраструктуры;
- оценка организации эксплуатации информационных технологий;
- оценка подготовки пользователей.

Технический аудит информационных технологий предполагает сбор и анализ информации, а также выдачу рекомендаций по улучшению работы отдельного технического элемента информационной инфраструктуры. При этом указанное направление аудита предполагает незначительный масштаб узкоспециализированных исследований.

Принципы аудита информационных технологий

Аудит ИТ-процессов – это аудит информационных технологий и систем, критичных для выполнения конкретного бизнес-процесса хозяйствующего субъекта с заданными критериями качества и эффективности. Одним из важнейших результатов этого направления аудита является формализованная модель исследуемого ИТ-процесса и конкретного бизнес-процесса. Выполнение указанного направления аудита предполагает:

- определение владельца бизнес-процесса;
- определение пользователей и участников бизнес-процесса;
- выявление применяемого оборудования и программных продуктов, участвующих в исследуемом ИТ-процессе;
- оценку действий обслуживающего персонала и пользователей ИТ-процесса;
- анализ проектных и регламентирующих документов.

При проведении аудита критерия информационных технологий осуществляется сбор и анализ информации, а также выдача управленческих рекомендаций по заранее определенному информационному критерию, например, безопасность, эффективность, доступность, соответствие требованиям и пр. В данном случае исследуются не только отдельный элемент информационной инфраструктуры, но и вся совокупность программных, аппаратных средств, процессов их сопровождения и обслуживания всего аудируемого субъекта.

И наконец, комплексный аудит информационной инфраструктуры предполагает определение и анализ взаимосвязей бизнес-процессов и их требований, информационных и смежных технологий, совокупности программно-аппаратных средств с целью выявления ее адекватности потребностям деятельности хозяйствующего субъекта. В настоящее время практической реализации указанных направлений аудита посвящен ряд международных регламентирующих документов. В них отражены вопросы практики аудирования, оценки рисков и надежности системы внутреннего контроля, технологические аспекты проведения аудита, учитывающие использование современных информационных технологий. При этом наиболее перспективным из них является постоянно развивающийся стандарт Cobit, который, вобрав в себя достижения значительного числа международных стандартов, легко масштабируется и наращивается. Стандарт Cobit позволяет использовать аудируемому субъекту любые разработки современных производителей аппаратно-программного обеспечения и исследовать информацию, не изменяя общепринятые подходы к аудиту и собственную структуру.

Принципы аудита информационных технологий

В ходе проведения аудита, основанного на стандарте Cobit, аудирующий субъект:

- содействует системе управления аудируемым субъектом в надлежащей организации управления информационными технологиями;
- осуществляет проведение периодических аудиторских исследований;
- помогает подготавливать внутренние нормативные документы;
- содействует предотвращению и смягчению сбоев информационных систем;
- участвует в управлении рисками, сопряженными с использованием тех или иных информационных технологий;
- осуществляет независимую интерпретацию управленческих рекомендаций по оптимизации функционирования информационной инфраструктуры аудируемого субъекта.

Таким образом, согласно требованиям стандарта Cobit основной целью аудита информационных технологий следует считать предоставление руководящему звену системы управления хозяйствующим субъектом обоснованных гарантий эффективного выполнения задач управления этими технологиями. Кроме того, тщательное аудиторское исследование информационных технологий способствует улучшению состояния информационной инфраструктуры, характеризующегося уровнем ее безопасности и эффективности управления. Поэтому в ходе аудита анализируется текущее состояние информационной инфраструктуры в целом и информационных технологий в частности и при выявлении существенных отклонений от определенных критериев производится оценка результирующих рисков и вырабатываются рекомендации по поводу требуемых корректирующих действий.

Модель анализа рисков по Cobit

Для оценки механизмов управления стандарт Cobit рекомендует использовать классическую модель аудиторского цикла. В соответствии с этой моделью критерии аудиторского исследования определяются стандартами или иными нормативными документами. Другим распространенным подходом практической реализации аудиторского исследования информационных технологий, основанным на требованиях стандарта Cobit, является модель анализа рисков, в которой критерии аудита формируются на основании оценки рисков.
Однако сами методы и подходы к анализу и управлению рисками, а также вопросы их использования при проведении аудита информационных технологий остаются за рамками указанного стандарта. В нем лишь даются их общие определения и краткие пояснения.

Модель анализа рисков по Cobit

Алгоритм модели анализа рисков начинается с оценки ИТ-ресурсов (Asset Valuation), необходимых для достижения бизнес-целей аудируемого субъекта. ИТ-ресурсы, как уже отмечалось ранее, включают в себя информацию, технические, программные и прочие средства (в том числе персонал), необходимые для ее получения, обработки, выдачи заинтересованным пользователям и хранения. На следующем этапе осуществляется анализ уязвимостей (Vulnerability Assessment) и угроз (Threat Assessment), препятствующих достижению бизнес-целей. Вероятность угрозы, величина уязвимости, а также размер возможного ущерба определяют степень риска, связанного с возможностью реального проявления той или иной угрозы. Далее аудитору необходимо выбрать корректирующие действия (контрмеры) (Counter Measures), оценить их эффективность (Control Evaluation), определить величину остаточных рисков (Residual Risk) после реализации контрмер и разработать для руководящего звена системы управления аудируемого субъекта план действий по внедрению механизмов управления (Action Plan).

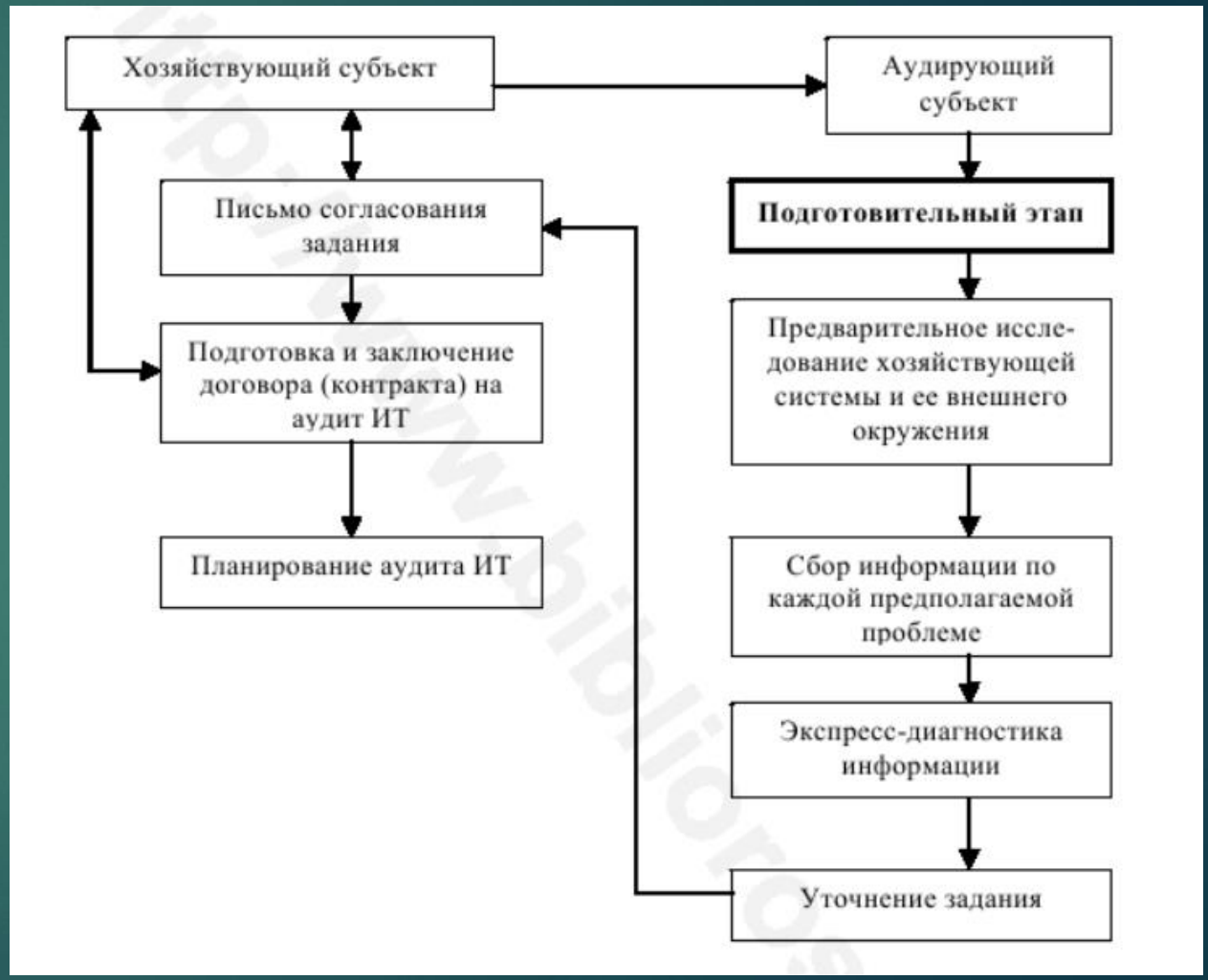
Классическая же модель аудиторского цикла, основанная на требованиях стандарта Cobit, опирается на концептуальное ядро Cobit, общие требования к аудированию ИТ-процессов (раздел Стандарта «Планирование и выработка стратегии аудита» и «Обобщенная схема руководства по аудиту») и общие принципы управления (раздел Стандарта «Общие замечания относительно оценки процессов управления»). Кроме того, Стандарт определяет и основные стадии проведения аудита и формулирует «Детальные инструкции по аудиту конкретных ИТ-процессов», которые являются лишь основой аудиторского исследования и требуют дополнения в каждом конкретном случае аудирования. Аудирующий субъект, приступая к аудиту конкретного хозяйствующего субъекта, должен учитывать, что стандарт Cobit служит лишь в качестве методологической основы разработки индивидуальных методик аудирования. В этой связи заслуживает особого внимания рассмотренная ранее модель аудиторского цикла операционного аудита, адаптированная на исследование информационных технологий и их взаимосвязей с деятельностью хозяйствующего субъекта.

Подготовительный этап анализа

Аудирующему субъекту, приступая к выполнению аудиторского задания, следует помнить, что каждый хозяйствующий субъект, являющийся его потенциальным клиентом, индивидуален и нетипичен. При этом его цели и ожидания также индивидуальны. Это, в свою очередь, требует особой тщательности и индивидуальности подхода к аудиторскому исследованию каждого из аудируемых субъектов. В общем понимании, планирование с точки зрения управления каким-либо видом деятельности или процессом способствует наиболее рациональному распределению работ и ресурсов, а также эффективному надзору за их выполнением и распределением. При этом надлежащее планирование аудиторской работы позволяет достичь понимания того, что всем значимым для аудируемого субъекта аспектам уделено должное внимание. Кроме того, тщательное планирование позволяет выявить и оценить наиболее существенные проблемы, стоящие перед этим субъектом, для того чтобы весь цикл аудирования был реализован в наиболее кратчайшие сроки и с минимальными затратами, а полученные при этом результаты были должным образом восприняты системой управления аудируемого субъекта и, как следствие, реализованы ею на практике. В то же время, принимая задание на проведение аудита информационных технологий, аудирующий субъект должен обозначить именно те проблемы, которые имеют наибольшее значение для данного конкретного хозяйствующего субъекта (его потенциального клиента). С этой целью важно осуществить подготовительный этап, то есть определить и согласовать с руководством этого субъекта конкретные цели и направления предстоящего аудиторского процесса. При этом основнаяроль руководства хозяйствующего субъекта, как заинтересованного в результатах аудита лица, состоит в том, чтобы оказывать всестороннюю поддержку аудирующему субъекту в уточнении формулировок наиболее значимых для него проблем, а также в подготовке достаточного и надлежащего информационного обеспечения предстоящего детального аудиторского исследования. Исходя из этого, указанный этап должен завершиться наиболее точной формулировкой основных проблем, стоящих перед хозяйствующим субъектом и требующих обязательного решения, а также заключением договора (контракта) на проведение аудита информационных технологий, согласно принимаемому аудирующим субъектом заданию. Иными словами, цель этого этапа – обеспечение единства в понимании предстоящего процесса аудирования как аудируемым, так и аудирующим субъектами.

Подготовительный этап анализа

Однако прежде чем заключить договор (контракт), аудирующий субъект должен, как было отмечено ранее, провести предварительное исследование всей хозяйственной системы (в том числе информационной инфраструктуры) и ее внешнего окружения, для того чтобы определить характер, временные рамки и масштаб предстоящего аудирования. При этом особо важными аспектами на подготовительном этапе являются сбор информации по каждой предполагаемой руководством хозяйствующего субъекта проблеме, а также экспресс-диагностика этой информации с целью выявления основных направлений детального аудиторского исследования по существу этих проблем. Указанный подготовительный этап следует завершить письмом согласования задания, подробно раскрывающим все аспекты предстоящего аудирования.
При этом следует учитывать, что если аудирующий субъект принимает задание от руководства хозяйствующего субъекта впервые, то указанное письмо должно быть особенно подробным. Если между субъектами уже существуют долгосрочные отношения по решению тех или иных проблем и реализации тех или иных заданий, то достаточно составлять короткое письмо, охватывающее только ключевые аспекты, которые будут решены в процессе предстоящего конкретного аудирования.



Подготовительный этап анализа

В общем виде письмо согласования задания может иметь произвольный характер. Однако в нем необходимо отразить:

- понимание проблем хозяйствующего субъекта аудирующим субъектом;
- цель и содержание аудирования;
- предметные области и объекты предстоящего исследования;
- общие методические подходы к предстоящему аудированию;
- форму отчетных документов;
- ответственность сторон;
- требования свободного доступа к любой информации, необходимой для проведения операционного аудита;
- требуемые ресурсы;
- краткое изложение ожидаемых результатов от выполнения задания.

Кроме того, в письмо согласования задания допустимо включать стратегические установки и проект общего плана предстоящего аудирования.

Так как указанное письмо является основой договора (контракта) между аудируемым и аудирующим субъектами, то, кроме указанных аспектов, в нем необходимо в краткой форме дополнительно раскрыть следующие не менее важные вопросы:

- ресурсы, которые обеспечивает аудируемый субъект (в том числе выделение специалистов по тем или иным предметным областям при возникновении в процессе аудирования необходимости);
- приблизительный график выполнения работ и ориентировочная продолжительность аудиторского цикла в целом, а также по отдельным этапам;
- общие принципы оплаты выполненных работ.

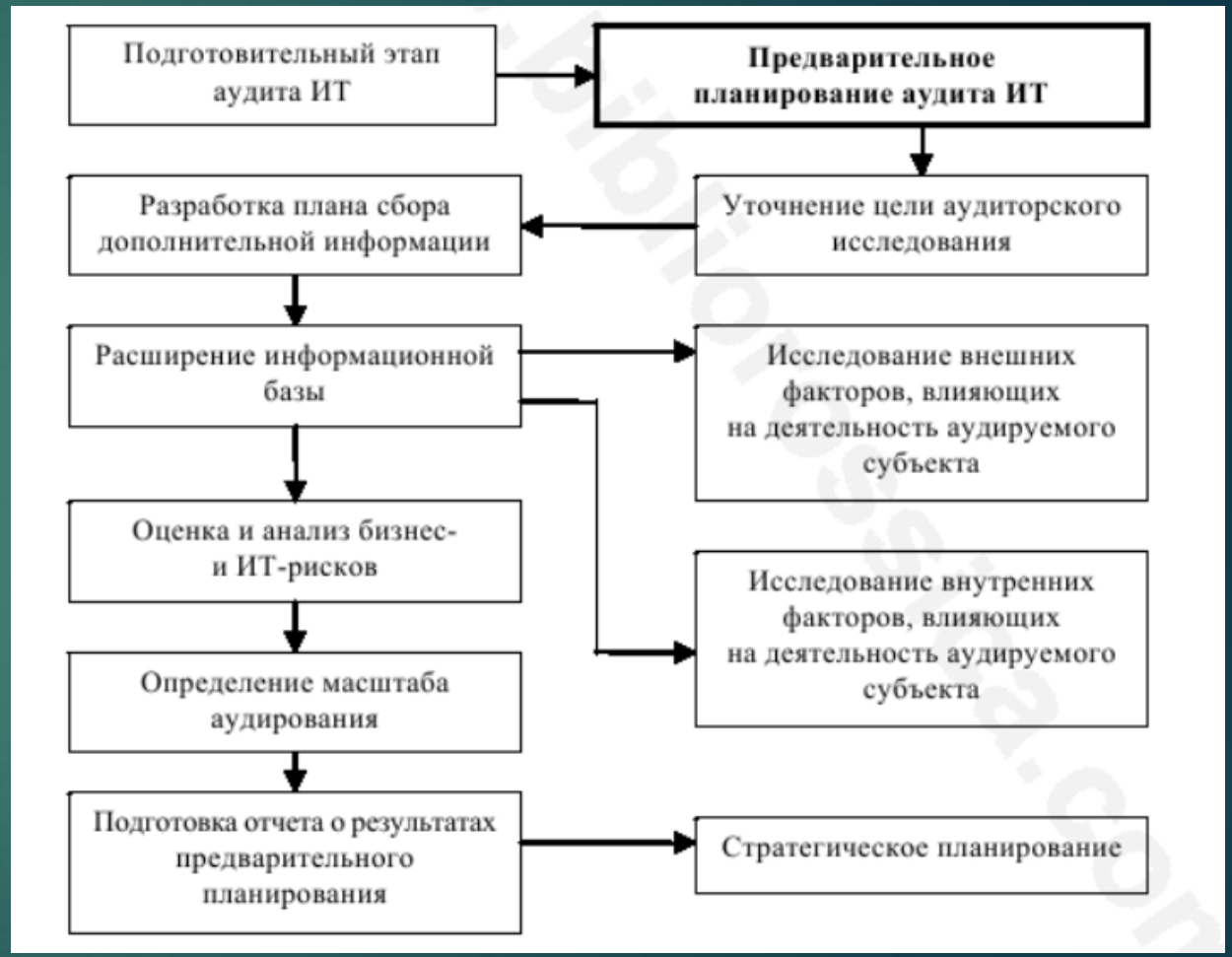
Этап заключения договра на аудит ИТ

Этап заключения договора (контракта) на проведение аудита информационных технологий, в свою очередь, требует достижения понимания сторонами предстоящего детального аудиторского исследования таких аспектов, как:

- сроки аудирования (в целом и по этапам);
- предметные области и объекты аудиторского исследования;
- условия конфиденциальности;
- количественный состав аудиторской группы с правом доступа к любой релевантной информации;
- количественный состав группы специалистов-экспертов;
- преемственность аудирования (при выполнении работ не впервые);
- состав, сроки и порядок представления аудирующему субъекту информации;
- состав, сроки, порядок и форма представления аудируемому субъекту как промежуточной аудиторской информации, так и результатов аудирования;
- сроки внедрения управленческих рекомендаций, полученных по результатам аудиторского исследования;
- условия мониторинга результатов реализации управленческих решений, выработанных на основе аудиторских рекомендаций;
- условия оплаты работ (в целом и по этапам);
- условия пересмотра договорной цены в ходе проведения аудирования (в случаях непредвиденных обстоятельств и дополнительно выявленных аспектов);
- условия расторжения договора (контракта) по желанию одной из сторон;
- прочие вопросы, включая дополнительные пожелания руководства аудируемого субъекта.

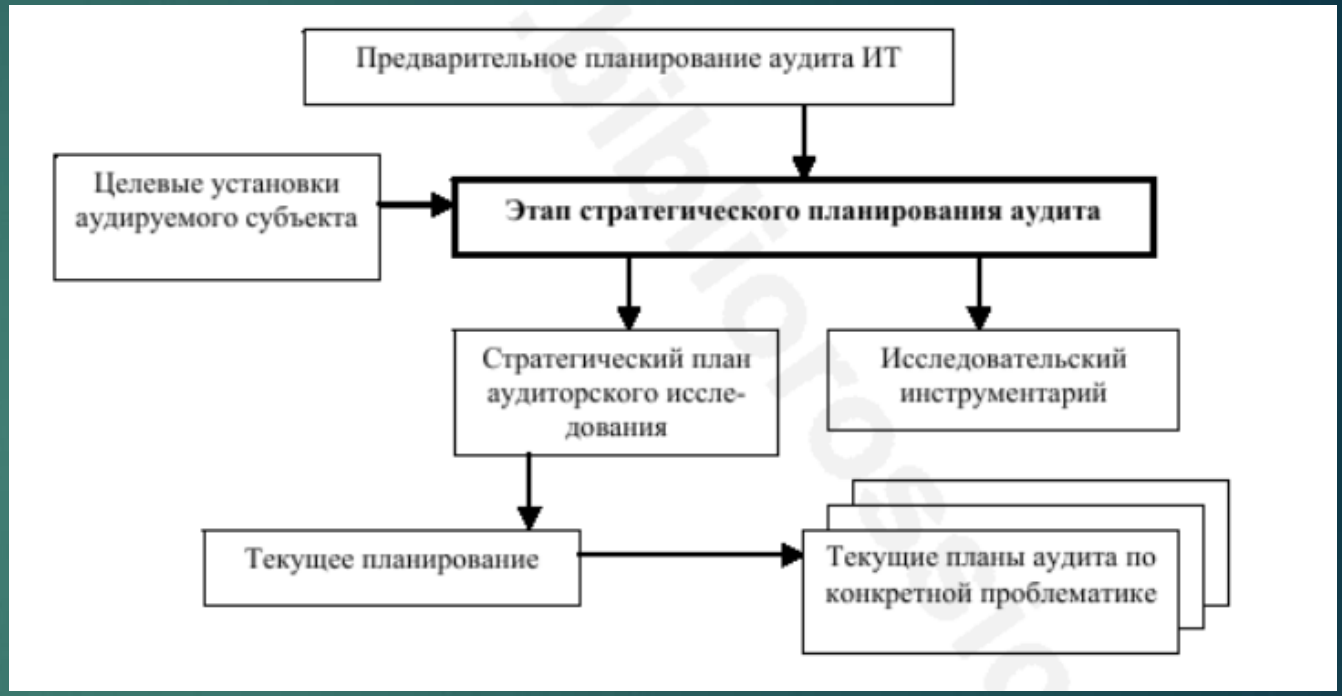
Предварительное планирование аудита ИТ

После подписания указанного документа, перед тем как будут выдвинуты начальные гипотезы и стратегические установки, а исследуемая проблема будет подвергнута декомпозиции на отдельные компоненты, что, в свою очередь, позволит определить наиболее значимые для них факторы, аудирующий субъект должен расширить свои знания об аудируемой хозяйственной системе и ее внешнем окружении. С этой целью необходимо тщательным образом переосмыслить деятельность аудируемого субъекта, для того чтобы определить и конкретизировать именно те направления сбора исходной информации, которые могут дать достаточные и надлежащие знания о стоящих перед ним проблемах. Расширяя и уточняя свои знания, полученные на подготовительном этапе, а также при проведении предыдущих исследований, на этапе предварительного планирования аудирующий субъект должен определить и оценить значительный объем всевозможных факторов и при этом выделить именно те из них, которые оказывают наибольшее влияние на эффективность развития аудируемой хозяйственной системы, и в частности информационной инфраструктуры.



Предварительное планирование аудита ИТ

Логическим завершением этапа планирования аудита информационных технологий любого хозяйствующего субъекта (независимо от формы его собственности) является разработка стратегической модели аудиторского исследования, а также текущих планов и программ на весь цикл предстоящего аудирования. Стратегическая модель аудита информационных технологий представляет собой совокупность планов, программ и методического инструментария, подготавливаемых аудирующим субъектом для выполнения аудиторского задания. Иными словами, стратегическая модель, разрабатываемая аудирующим субъектом на этапе стратегического планирования, представляет собой общий стратегический план всего аудиторского исследования, согласующийся с целевой направленностью деятельности аудируемого субъекта или принятого конкретизированного аудиторского задания, выявленными на предварительном этапе планирования проблемами, стоящими перед аудируемым субъектом, возможностями их решения и преодоления, а также предполагаемого для применения на всем протяжении аудиторского цикла исследовательского инструментария.



Тестирование аудирующего субъекта

После завершения этапа планирования и формирования стратегической модели аудита информационных технологий аудирующий субъект приступает к аудированию по существу. Согласно требованиям стандарта Cobit, процедура аудита по существу включает в себя четыре последовательных этапа:

- идентификация и документирование, т.е. сбор и первичный анализ информации, дополняющей и расширяющей знания, полученные на этапе планирования и формирования стратегической модели;
- оценка механизмов управления;
- тест соответствия;
- детальное тестирование.

На этапе идентификации и документирования осуществляется документирование и идентификация существующих механизмов управления посредством интервьюирования руководящего звена системы управления аудируемым субъектом, отдельных компетентных ИТ-специалистов, специалистов по управлению рисками и основных пользователей ИТ-сервисов с целью получению или уточнения знаний относительно:

- требований деятельности аудируемого субъекта и связанных с ней рисков;
- организационной структуры;
- распределения ролей и ответственности; политик и процедур, имеющих отношение к оценке рисков; страхования остаточных рисков и пр.;
- требований нормативной базы;
- существующих механизмов управления;
- существующей отчетности.

На этапе оценки механизмов управления аудирующий субъект осуществляет оценку эффективности существующих у аудируемого субъекта механизмов управления при выполнении задач управления, их целесообразность и адекватность. При этом осуществляется сравнение существующих механизмов управления с установленными критериями, требованиями технических стандартов и критическими факторами успеха. В свою очередь, стандарт Cobit предполагает, что, для того чтобы модель управления работала надлежащим образом, необходимо четко распределить ответственность за бизнес-процессы, установив при этом строгую подотчетность каждого должностного лица.

Тестирование аудирующего субъекта

На этом этапе аудитор должен убедиться в том, что существующие ИТ-процессы надлежащим образом задокументированы, а ответственность и подотчетность четко определены. Кроме того, аудитор должен по необходимости предусмотреть и разработать компенсирующие механизмы управления. Для получения гарантий пригодности существующих у аудируемого субъекта механизмов управления для решения задач управления аудитор должен провести тесты соответствия. Тестирование осуществляется посредством получения прямых и косвенных свидетельств надлежащего выполнения установленных процедур управления за исследуемый период. Кроме того, на этом этапе аудирования по существу выполняется ограниченное исследование пригодности результатов процессов управления, а также определяется уровень детального тестирования и объем дополнительных процедур, необходимых для получения гарантий адекватности ИТ-процессов. Согласно требованиям стандарта Cobit, оценку механизмов управления необходимо осуществлять путем исследования следующих утверждений:

- существование надлежащей структуры систематической оценки рисков (включая риски недостижения целевых установок), а также системы управления этими рисками;
- подходы к анализу рисков предусматривают регулярность обновления оценок на всех уровнях управления;
- существующие процедуры оценки рисков позволяют учитывать как внешние, так и внутренние факторы, а также учитывают результаты аудитов, ожидания и идентифицированные инциденты;
- целевые установки хозяйствующего субъекта включены в процесс идентификации рисков;
- процедуры мониторинга изменений в работе систем аудируемого субъекта предусматривают своевременное уточнение данных о системных рисках и уязвимостях;
- существование процедур непрерывного мониторинга и улучшения оценки рисков, облегчающее процессы создания надлежащих механизмов управления (в частности, оперативного операционного аудита);
- включены ли в процедуру идентификации рисков вероятность, частота и методы их анализа;
- включает ли в себя документация по оценке рисков описание методологии этой оценки, идентификацию существенных уязвимостей и соответствующих рисков;
- адекватна ли квалификация персонала, выполняющего оценку рисков.

Тестирование аудирующего субъекта

И наконец, детальное тестирование механизма управления предполагает оценку и обоснование рисков невыполнения задач управления посредством применения аналитических и эвристических методов (в частности, методов экспертных оценок). Целью указанного этапа является побуждение высшего звена системы управления аудируемым субъектом к выполнению выработанных по результатам аудиторского исследования корректирующих воздействий по улучшению состояния системы управления информационными технологиями. На данном этапе аудирующий субъект производит документирование свидетельств всех недостатков механизмов управления, угроз и уязвимостей, являющихся следствием этих недостатков, реальных и потенциальных последствий угроз. При этом инструментом указанного исследования служит сравнительный и причинно-следственный анализ. После завершения указанных этапов аудирующий субъект формулирует выводы и управленческие рекомендации. Результаты аудита информационных технологий обычно классифицируют по трем основным группам:

- организационная: планирование, управление, документооборот функционирования информационной инфраструктуры;
- техническая: сбои, неисправности, оптимизация работы элементов информационной инфраструктуры, непрерывное обслуживание, модернизация инфраструктуры и т.д.;
- методологическая: подходы к решению проблемных ситуаций, управлению и контролю, общая упорядоченность и структуризация.

Таким образом, проведенный аудит информационных технологий позволяет обосновать:

- долгосрочный план развития информационной инфраструктуры аудируемого субъекта;
- политику безопасности;
- методологию работы и доводки информационных технологий;
- план восстановления информационной инфраструктуры в чрезвычайных ситуациях.

Перечень указанных выгод проведения аудита информационных технологий не окончателен и в каждом конкретном случае аудирования может быть значительно расширен.

Спасибо за внимание!