ИНФОРМАЦИОННЫЙ АУДИТ И ИНФОРМАЦИОННЫЕ РИСКИ

© Завгородний В.И.[♣]
Финансовый университет при Правительстве Российской Федерации,
г. Москва

Анализируются различные подходы к пониманию сущности информационного аудита, соотношение и взаимосвязь информационного аудита и анализа информационных рисков.

В настоящее время нет общепризнанного научного определения информационного аудита. Часто под информационным аудитом понимают аудит отдельных составляющих информационных систем и направлений управления такими системами. Так информационным аудитом называют аудит информационной безопасности, аудит информационных ресурсов и информационных потоков, аудит соответствия состояния информационных технологий и средств задачам их применения. В Российской Федерации пока еще не создана законодательная база информационного аудита и соответствующие стандарты, хотя научно-практическая работа в этом направлении ведется.

Информационный аудит и управление информационными рисками

Наибольшее признание понимания сущности информационного аудита получил подход, представленный в документах COBIT (Control Objectives for Information and Related Technology), имеющих статус международного стандарта де-факто. Современные версии COBIT разработаны Институтом управления информационными технологиями (IT Governance Institute), учрежденным Ассоциацией аудита и контроля информационных систем (Information Systems Audit and Control Association, ISACA). В 2011 г. должна быть завершена работа над пятой версией стандарта COBIT. В действующей версии стандарта требования к организации информационного аудита изложены в книге Руководство по аудиту (Audit Guideline).

Методология Руководства по аудиту направлена на получение информации о состоянии информационной сферы предприятия и результатах воздействия ее на основные бизнес-процессы. В соответствии с подходом стандарта COBIT цель информационного аудита состоит в системной оценке эффективности применения информационных технологий (ИТ) и рисков, связанных с использованием этих технологий в деятельности предприятия. Такой аудит проводится в интересах, прежде всего, первых лиц предприятия для принятия на его основе решений по перспективам развития информаци-

[♣] Профессор кафедры «Информатика и программирование», доктор экономических наук, доцент.

онных технологий и их интеграции с производственными процессами. Стандарт рассчитан также на менеджеров бизнес-процессов, менеджеров ИТ служб и аудиторов.

Руководство предприятия, в зависимости от целей проведения информационного аудита, может возлагать на него решение следующих задач:

- определение интегральной эффективности применения ИТ-технологий на предприятии;
- получение данных об эффективности отдельной информационной технологии (внедренной или планируемой к использованию);
- оценка всех информационных рисков предприятия или информационных рисков, связанных с определенными ИТ;
- определение соответствия системы управления ИТ-процессами требованиям стандартов.

В COBIT определены 7 требований к информации, используемой в бизнес-процессах: полезность, эффективность, конфиденциальность, достоверность, целостность, доступность, соответствие требованиям.

Полезность характеризует значимость информации для бизнес-процессов, а также получение ее регулярно, корректно, последовательно и в удобном виде. Эффективность характеризует получение информации посредством оптимального (наиболее продуктивного и экономичного) использования ресурсов. Конфиденциальность имеет отношение к защите важной информации от несанкционированного раскрытия. Достоверность информации предполагает ее соответствие реальному состоянию объектов. Целостность связана с точностью и полнотой информации, а также с ее обоснованностью в соответствии с корпоративными ценностями и ожиданиями. Доступность характеризует возможность получения своевременного доступа к информации, в соответствии с временными требованиями бизнес процесса. Соответствие требованиям выражается в соответствии законам, регулирующим актам и условиям контрактов, для которых бизнес-процесс является субъектом, то есть внешним требованиям к бизнесу, равно как и внутренней корпоративной политике.

Анализ приведенных требований показывает, что они могут быть представлены тремя группами требований к бизнес-информации – требования эффективности, качества и безопасности. Общепринято безопасность информации определять характеристиками целостности, конфиденциальности и доступности. Из приведенного перечня к требованиям качества информации могут быть отнесены: полезность, достоверность, соответствие требованиям.

Безопасность информации обеспечивается в процессе управления информационными рисками. В настоящее время все большее распространение находит подход к пониманию информационных рисков, в соответствии с которым информационные риски связываются не только с безопасностью, но и с качеством информации.

Тогда управление информационными системами (информационной сферой предприятия) может быть представлено как управление эффективностью системы и информационными рисками. Интегральная эффективность системы может оцениваться как разница положительного эффекта от использования информационных технологий и ущерба от реализации рисковых событий в информационной сфере. Интегральная эффективность информационной системы может быть оценена в денежном представлении или в относительных единицах (например, ROI).

Интегральная оценка эффективности информационных систем за определенный период времени (например, за год) позволяет наиболее полно и точно оценить уровень управления информационной сферой предприятия. Она позволяет определить экономический эффект от использования информационных технологий на конкретном предприятии, с учетом всех его особенностей и внешних условий. Однако использование такой оценки на практике связано с целым рядом трудностей. Основными из них являются сложность выделения доли положительного эффекта, полученного от применения информационных технологий, из общего положительного результата работы предприятия, а также сложность определения ущерба предприятия от информационных рисков. Получение такой характеристики связано не только с методологическими трудностями, но и с большими трудозатратами. Кроме того, такой показатель сложно использовать для сравнения результатов управления информационной сферой различных предприятий, определить степень соответствия управления лучшим мировым практикам.

Поэтому на практике аудит информационной сферы ориентирован на проверку соответствия системы управления информационной сферой предприятия требованиям системы стандартов. В иерархии стандартов, получивших международное признание, стандарт COBIT относится к стандартам верхней иерархии, положения которого развиваются в других стандартах и лучших практиках, таких как ITIL, ISO/IEC 20000 и др.

В Руководстве по аудиту определяются правила использования концептуального ядра и основных принципов управления COBIT при проведении информационного аудита. Оно содержит описание проверки реализации 34 высокоуровневых ИТ-процессов и 318 детальных задач управления, определенных в концептуальном ядре COBIT. Это позволяет аудитору оценивать адекватность реализованной системы управления ИТ требованиям стандарта и бизнес-целям и формировать рекомендации по ее улучшению.

Цели и показатели эффективности (метрики) определяются в COBIT на трех уровнях:

- цели и показатели эффективности ИТ, которые определяют вклад ИТ в достижение бизнес целей и позволяют его измерить;
- цели и показатели эффективности ИТ-процесса, которые определяют, что является вкладом ИТ процесса в достижение ИТ-целей и способы измерения;

– цели и показатели эффективности отдельных видов деятельности (действий, функций), которые определяют внутреннее содержание ИТ-процесса для достижения требуемой эффективности и методы измерения.

Процедуры аудита, включают в себя четыре последовательных этапа:

– идентификацию и документирование (включает в себя сбор и первичный анализ информации);
– оценку механизмов управления;
– тест соответствия;
– детальное тестирование.

На этапе идентификации и документирования осуществляется документирование процедур и идентификация существующих механизмов управления путем интервьюирования руководства и сотрудников организации с целью уяснения следующих вопросов:

– требования бизнеса и ассоциированные с ними риски;
– организационная структура;
– распределение ролей и ответственности;
– политики и процедуры;
– требования нормативной базы;
– существующие механизмы управления;
– существующая отчетность.

На этапе оценки механизмов управления оценивается эффективность существующих механизмов управления при выполнении задач управления, оценивается их целесообразность и пригодность путем сравнения с установленными критериями, промышленными стандартами и критическими факторами успеха. При помощи методов экспертных оценок определяется для каких механизмов управления на следующем этапе должно быть протестировано соответствие установленным процедурам Аудитору необходимо убедиться в том, что:

– существующие ИТ-процессы документированы;
– ответственность и подотчетность четко определены;
– в необходимых случаях существуют компенсирующие механизмы управления.

Тестом соответствия называется этап аудита, задачей которого является контроль пригодности существующих механизмов управления для решения задач управления. Проверка осуществляется путем получения прямых и косвенных свидетельств надлежащего выполнения установленных процедур управления за оцениваемый период. На этом этапе выполняется также ограниченное исследование адекватности результатов процессов управления, определяется уровень детального тестирования и объем дополнительной работы, необходимой для получения гарантий адекватности ИТ-процесса.

Детальным тестом называется заключительный этап аудита, целью которого является оценка и обоснование рисков невыполнения задач управ-

ления путем использования аналитических методов и экспертных оценок. Конечная цель этапа заключается в том, чтобы убедить руководство в необходимости изменения механизмов управления для улучшения состояния системы управления ИТ организации. На данном этапе аудитор производит документирование недостатков механизмов управления, угроз и уязвимостей, являющихся следствием этих недостатков, реальных и потенциальных последствий реализации рисков путем причинно-следственного анализа и проведения сравнительного тестирования.

* * *

Использование методологии COBIT для проведения аудита информационной сферы предприятия позволяет получить полную информацию о степени соответствия процессов управления информационными технологиями целям бизнес-процессов и требований стандартов, оценить информационные риски. Аудит обеспечивает выявление недостатков в управлении информационными технологиями и определение направления совершенствования управления.

Использование методологии COBIT для проведения информационного аудита сопряжено с рядом трудностей. Стандарт определяет лишь требования к процедурам управления информационными технологиями, не касаясь непосредственных механизмов ИТ-процессов. Поэтому необходимо руководствоваться другими стандартами и лучшими практиками. Внедрение методологии COBIT в полном объеме является трудоемкой задачей и ее полное внедрение возможно только в больших компаниях. Для малых и средних предприятий могут использоваться отдельные положения стандарта. Трудности использования методологии заключаются также в большом объеме документов COBIT (количество книг исчисляется десятками). К тому же на русский язык переведены только отдельные документы, отдельные англоязычные термины не имеют адекватного перевода.

Список литературы:

1. Стандарт COBIT.

2. Завгородний В.И. Системное управление информационными рисками. Выбор механизмов защиты от информационных рисков // Проблемы управления. – 2009. – № 1.