Введение

Современные информационные технологии составляют неотъемлемую часть производственной инфраструктуры, обеспечивая выполнение жизненно важных для функционирования предприятий бизнес-процессов. Информационные технологии и системы не только поддерживают бизнес-процессы предприятия, но и должны обеспечивать целый ряд дополнительных характеристик, таких, как безопасность информации, удобство использования, непрерывность функционирования и пр. Создание качественных ИТ-решений должно основываться на использовании методологий и лучших практик, охватывающих все этапы жизненного цикла систем – от планирования ИТ-стратегии до организации эксплуатации установленных приложений и систем. Однако на практике зачастую отказываются от выполнения каких-то правил и процедур в угоду сокращению сроков проектов и стоимости систем.

Аудит информационных технологий (ИТ-аудит) решает задачу получения актуальной и достоверной информации о текущем уровне качества функционирования системы. Результаты аудита могут служить объективной основой для формирования рекомендаций по повышению эффективности функционирования всей ИТ-инфраструктуры предприятия.

Обычно ИТ-аудит проводится перед принятием решений о создании или модернизации информационных систем, в случаях неудовлетворительной работы информационных систем, при возникновении сомнений в качестве услуг аутсорсинга, при разработке или модернизации системы обеспечения информационной безопасности организации.

Опыт применения процедур аудита и их результатов показывает, что они обеспечивают достижение следующих результатов:

- Снижение затрат на эксплуатацию информационных систем.
- Повышение производительности информационных систем.
- Повышение надёжности информационных систем.
- Обеспечение безопасности информационных систем.
- Повышение эффективности взаимодействия распределенных подразделений компании и снижение коммуникационных затрат.

В процессе аудита производится обследование и оценка разнообразных аспектов применения информационных систем в организации, которые обычно включают в себя:

- Организацию руководства информационными системами и технологиями в компании.
- Принятые в компании процедуры управления жизненным циклом информационных систем.
- Организацию эксплуатации и сопровождения ИТ-сервисов.

- Характеристики сетевой инфраструктуры.
- Процедуры обеспечения защиты информационных активов компании.
- Обеспечение непрерывности бизнеса и восстановления систем после аварий и катастроф.

ИТ-аудит осуществляется в рамках достаточно сложных проектов, которые требуют от исполнителей как глубоких знаний различных аспектов информационных технологий и систем, так и понимания принципов и технологии организации аудита, методик проведения проверок и оценки получаемых результатов. Поэтому подготовка ИТ-аудитора оказывается сложной задачей, связанной с формированием у специалиста множества разнообразных компетенций.

Признанным лидером в области ИТ-аудита в настоящее время является международная ассоциация ISACA (The Information Systems Audit and Control Association), разработавшая собственный набор стандартов и обязательных требований к содержанию и организации ИТ-аудита.

Стандарты ISACA охватывают все основные аспекты ИТ-аудита:

- Стандарт S1 (Audit Charter) определяет содержание и требования к основному рабочему документу – уставу проекта аудита.
- Стандарт S2 (Independence) определяет требования к независимому статусу аудитора.
- Стандарт S3 (Professional Ethics and Standards) определяет принципы профессиональной этики аудитора и требования по применению стандартов при осуществлении аудита.
- Стандарт S4 (Professional-Competence) фиксирует требования к профессиональной подготовке аудитора.
- Стандарт S5 (Planning). описывает лучшие практики планирования проектов аудита, основанных на анализе рисков.
- Стандарт S6 (Performance of Audit Work) определяет требования к качеству аудита.
- Стандарт S7 (Reporting) является руководством по подготовке отчетности по аудиту.
- Стандарт S8 (Follow-up Activities) определяет обязанности аудитора по контролю за принимаемыми заказчиком мерами по реализации рекомендаций аудита.
- Стандарт S9 (Irregularities and Illegal Acts) содержит рекомендации аудитору по выявлению нарушений и недопустимых действий.
- Стандарт S10 (IT Governance) содержит рекомендации по оценки процедур руководства информационными технологиями в компании.
- Стандарт S11 (Use of Risk Analysis in Audit Planning) определяет требования к применению методик анализа рисков при планировании проекта аудита.

- Стандарт S12 (Audit Materiality) представляет рекомендации по оценке значимости недостатков в процессах управления.
- Стандарт S13 (Using the Work of Other Experts) содержит рекомендации по использованию в процессе аудита заключений сторонних экспертов.
- Стандарт S14 (Audit Evidence) содержит требования к качеству данных и доказательств, плучаемых в процессе аудита.

Ряд стандартов регламентирует проверку конкретных областей управления информационными технологиями или учитывает применение информационных технологий в специфических областях деятельности.

- Стандарт S15 (IT Controls) является руководством по оценке жизненного цикла процессов управления ИТ в компании.
- Стандарт S16 (E-Commerce) содержит рекомендации по организации оценок ИТ, используемых с среде электронного бизнеса.

Стандарты сопровождаются руководствами по их применению.

В настоящем учебном пособии рассматривается организация проекта аудита и основные задачи, которые должен выполнять аудитор информационной системы на различных этапах проекта. В книге приводятся базовые сведения о практиках и технологиях, применяемых в компаниях для организации и поддержки ИТ, на соответствие которым осуществляются проверки. В списке литературы даны ссылки на источники, содержащие подробные описания лучших практик управления.

При необходимости получения более детальных сведений по процессу аудита можно рекомендовать использование оригинальных документов ISACA [1]. Курс базируется на материалах, рекомендованных ISACA для подготовки сертифицированных аудиторов информационных систем [2, 3].

Изучение материала книги обеспечивает формирование необходимых компетенций для выполнения всестороннего аудита информационных технологий предприятия. В результате изучения курса студент будет:

Знать: предмет и цели проведения аудитов различного вида; методику организации проектов аудита; основные положения, принципы и современные практики управления информационными активами предприятия.

Уметь: формировать планы аудиторских проверок; выбирать необходимые методы для проведения тестирования и контрольных проверок; анализировать и интерпретировать результаты аудита; готовить отчетность по проекту аудита,

Владеть: методами сбора информации при проведении аудита; методами оценки состояния информационных систем и связанных с ними процессов; методиками формирования заключений по результатам проверок.