УДК 004.09

НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ АУДИТА ИНФОРМАЦИОННЫХ СИСТЕМ  
  
Юдаев И.А., Андрианова Е.Г.

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА — Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78,   
e-mail:dtghmflysq@gmail.com

Особенностью функционирования аудируемого предприятия сегодня является постоянный рост требований, предъявляемых пользователями к обработке финансовой информации. Рассмотрены основные стандарты, используемые при аудите информационных систем. Описаны этапы аудита информационных систем.

Ключевые слова: аудит информационных систем, CoBiT.

AREAS FOR IMPROVEMENT IN THE AUDIT OF INFORMATION SYSTEMS  
  
Yudaev I.A., Andrianova E.G.

Federal State Budgetary Educational Institution of Higher Education "MIREA - Russian Technological University", 119454, Russia, Moscow, 78 Vernadsky Avenue, e-mail:dtghmflysq@gmail.com

A feature of the functioning of the audited company today is the constant growth in the requirements set by users for processing financial information. The main standards used in the audit of information systems have been reviewed. The stages of information systems audit have been described.

Keywords: information systems audit, CoBiT.

**Введение**

В настоящее время проблема совершенствования и развития методологического аппарата ИТ аудита связана с необходимостью повышения его качества в целях удовлетворения потребностей общества в достоверной информации о финансовом состоянии организаций, а также с использованием в этих целях современных информационных технологий. Особенностью функционирования аудируемого предприятия сегодня является постоянный рост требований, предъявляемых пользователями к обработке финансовой информации. Важным фактором использования информационных систем в учетной деятельности является снижение трудозатрат по обработке информации и повышения скорости получения результатных данных. От эффективности функционирования информационных систем непосредственно зависит устойчивое развитие предприятия при значительно возросшем уровне автоматизации учетной деятельности.

С учетом все возрастающей зависимости проверяемых организаций от их информационных систем возникает необходимость в дальнейшем совершенствовании аудиторских стандартов в области планирования и осуществления аудита и оценки риска и внутреннего контроля в компьютерной среде и информационных систем аудируемого субъекта. Необходимо отметить то, что компьютерная обработка данных является не столько формализованной технической процедурой, сколько средой, в которой осуществляются процессы сбора, обработки, трансформации и хранения информации. Компьютерная обработка данных представляет собой совокупность технических процессов, в которой формируются информационные потоки, т.е. формируется среда, которая является условием функционирования информационных систем.

Использование информационных систем (ИС) в учетной деятельности приводит к возникновению рисков, которые не характерны обработке данных вне компьютерной среды, например, риск неоднократного ввода данных, риски сохранности информации, риски хакерских атак и т.д. Влияние указанных рисков в среде компьютерной обработки данных увеличивается вследствие их узкой специфичности.

В связи с этим возникает необходимость исследования и уточнения понятийного аппарата, создание методики проверки и стандартизация такой специфической области, как информационный аудит, а также работы по совершенствованию информационных систем аудита, что требует дальнейшего исследования этой предметной области.

В последние годы большое внимание уделяется аудиту эффективности информационных систем. В данном направлении в международной практике были разработаны стандарты CobiT, Information technology infrastructure library (ITIL), Capability Maturity Model Integration (CMMI), Committee of sponsoring organizations (COSO).

Методика аудита информационных систем рассматривается преимущественно в технических аспектах функционирования информационных систем, влияющих на составление отчетности компании. В настоящее время отсутствует единая позиция о сущности аудита информационных систем. Методика аудита информационных систем, влияющих на достоверность составления отчетности, практически не разработана.

Исходя из этого, сегодня весьма актуальной является задача разработки методики ИТ аудита в условиях компьютерной обработки данных и практических аспектов ее применения. Недостаточная разработанность концептуальных и методологических подходов к аудиту информационных систем определили выбор темы и направление исследования.

**Общие положения и стандарты к проведению ИТ-аудита**

Общие тенденции глобализации в индустрии приводят к ускорению и усложнению развития бизнес-процессов организации. И как следствие, информационная инфраструктура предприятий становится важнейшим условием, непосредственно влияющим на эффективность деятельности организации. Информационная структура является комплексом структур, которая обеспечивает функционирование и развитие информационного пространства, а также средств информационного взаимодействия. Она включает в себя не только совокупность информационных центров, баз данных и знаний, но также обеспечивает доступ потребителей к информационным ресурсам [1].

В данной работе разрабатывается методология проведения ИТ-аудита для предприятия среднего бизнеса. Методология основывается на передовых стандартах и подходах в области организации, управления и обеспечения безопасности ИТ-инфраструктуры, а именно:

Cobit, Control Objective in IT and related technologies (Цели контроля в ИТ и смежных технологиях).

COSO – стандарт управления рисками организаций. Разработан Комитетом спонсорских организаций Комиссии Тредвея в 2004 г.

СТ РК ИСО/МЭК 17799, Свод правил по управлению защитой информации.

Internal Control Guide DTTL (руководство к проведению оценки внутреннего контроля организации от компании Делойт).

**COBIT – контрольные объекты информационных технологий**

Открытый стандарт CoBiT был разработан с целью помощи аудиторам и консультантам, руководителям отделов информационно-технической поддержки, администраторам и заинтересованным пользователям ассоциацией ISACA, а также привлеченными специалистами из ведущих мировых консалтинговых компаний. Первое издание стандарта было сформировано в 1996 году было продано в 98 странах, что значительно облегчило работу профессиональных аудиторов в сфере информационных технологий. Стандарт (рис. 1) связывает информационные технологии и действия аудиторов, объединяет и согласовывает многие другие стандарты в единый ресурс, который позволяет получить адекватное представление о целях и задачах информационной системы, учитывая все особенности информационных систем различного масштаба и сложности.

В основе стандарта CoBiT заключается то, что ресурсы информационной системы должны управляться набором процессов, сгруппированных естественным образом для обеспечения Компании требуемой и надежной информацией. Основные ресурсы и критерии их оценки, используемые в стандарте CoBiT:

1. Люди – под данными ресурсами понимаются не только сотрудники организации, но также ее руководство и контрактный персонал. Рассматриваются навыки штата, понимание им задач и производительность его работы.
2. Приложения - производственное ПО.
3. Технологии - аппаратные средства, операционные системы, базы данных, системы управления информационной системой и т. д.
4. Оборудование - все аппаратные средства информационной системы организации с учетом их обслуживания.
5. Данные - внешние и внутренние, структурированные и не структурированные, графические, звуковые и т. д.

Все эти ресурсы оцениваются CoBiT на каждом из этапов построения или аудита информационной системы по следующим критериям:

* эффективность - уместность информации и ее соответствие задачам бизнеса;
* технический уровень - соответствие стандартам и инструкциям;
* безопасность - защита информации;

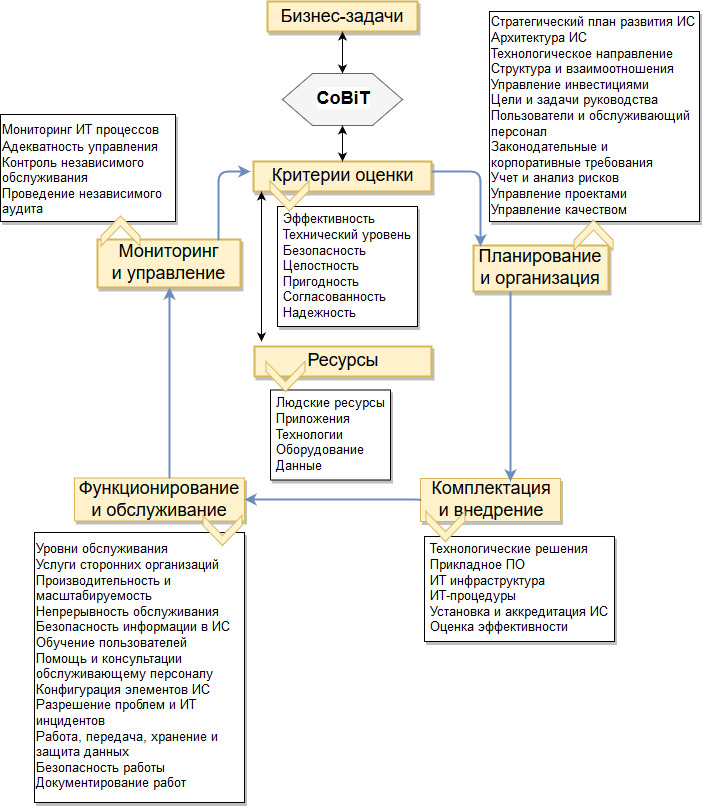


Рисунок 1. Структура стандарта CoBiT

* целостность - точность и законченность информации;
* пригодность - доступность информации, потребной для бизнес-процессов в настоящем и будущем, защита необходимых и сопутствующих ресурсов;
* согласованность - исполнение законов, инструкций и договоренностей, влияющих на бизнес-процесс, т. е. внешних требований к бизнесу;
* надежность - достоверность информации, предоставляемой руководству организации, осуществление соответствующего управления финансированием и согласованность должностных обязанностей.

CoBiT базируется на стандартах аудита ISA и ISACF, но включает и другие международные стандарты, в том числе принимая во внимание все утвержденные ранее стандарты и нормативные документы: технические стандарты, кодексы, профессиональные стандарты, требования и рекомендации, требования к банковским услугам, системам электронной торговли и производству.

**Аудит информационной системы**

Подход к предоставлению аудита информационной системы как отдельной самостоятельной услуги с течением времени упорядочился и стандартизировался. Крупные и средние консалтинго-аудиторские компании образовали ассоциации - союзы профессионалов в области аудита информационных систем, которые занимаются созданием и сопровождением стандартов аудиторской деятельности в сфере ИТ. Ассоциация ISACA занимается непосредственно открытой стандартизацией аудита информационных систем. Основная декларируемая цель ассоциации – исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

Необходимость аудита информационных систем и баз данных обусловлена, прежде всего, широким распространением ИТ в области финансового учета и усложнением процессов обработки информации.

Одной из главных задач ИС компании или предприятия является создание различных отчетов, в частности финансовой отчетности. Данные отчеты позволяют менеджменту предприятия своевременно отслеживать течение бизнес-процессов во всей организации, оценивать их эффективность, прогнозировать результаты хозяйственной деятельности.

В ходе аудита ИС проводится анализ ее структурных компонентов, посредством разделения на составные части и отбора ключевых элементов, оказывающих на формированные достоверной информации наибольшее влияние. При этом учитываются все изменения, произведенные Компанией в структуре ИС в соответствии с его стратегическими задачами развития.

Для понимания процессов аудита ИС необходимо рассмотреть ее структуру, которая независимо от вида ИС будет содержать ядро, которое остается неизменным (Рис. 2).

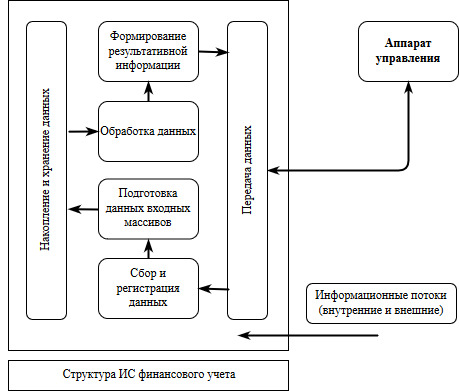


Рисунок. 2. Структура информационный системы финансового учета

В ИС крупного масштаба, таких как ИС в корпоративной системе управления или в интегрированных системах финансового учета, основные элементы могут дополняться более сложными структурными единицами.

Так бухгалтерская ИС в комплексной системе управления компании также взаимодействует с другими ИС - система маркетинга, система финансовой планирования, система оперативного управления производством, система анализа финансовой и хозяйственной деятельности, кадровая система, система делопроизводства и электронного документооборота.

В ходе аудита ИС рассматриваются следующие важные вопросы:

* наличие стратегического плана развития информационной инфраструктуры экономического субъекта, отдельного от общей стратегии предприятия;
* наличие контрольных процедур в отношении отчетов, которые ИС предоставляет менеджменту экономического субъекта;
* наличие контрольных процедур в отношении проверки качества внутренней и внешней информации, используемой в работе ИС;
* наличие формализованного процесса учета хозяйственных операций.

ИС призваны хранить данные обо всех хозяйственных операциях компании (дату совершения, сумму, контрагента, описание операции), проводить их правильную классификацию по указанным параметрам, таким образом, чтобы информация в финансовой отчетности не была искажена.

В ходе аудита ИС происходит ее всестороннее тестирование, строятся схемы зависимостей и потоков информации, сравниваются требуемые и фактические показатели функционирования ИС, анализируется полученные данные.

Таким образом, проводится комплексная оценка ИС, позволяющая оценить воздействие нарушений и сбоев в ее работе на достоверность формируемой отчетности, а также резервов ее более эффективного использования.

В данном случае аудит ИС выступает в качестве средства приведения ИС компании в соответствие с его бизнес-целями. Также аудит ИС позволяет избежать непрогнозируемого развития и изменения ее характеристик.

Использование компанией или предприятием информационных технологий в ходе проведения внутренних контрольных процедур повышает их эффективность и скорость.

Однако это может привести к появлению определенных рисков, влияющих на целостность и безопасность финансовой информации. Ниже приведены преимущества от использования ИС и возможные риски.

Таблица 1. Преимущества и риски от использования информационных систем

|  |  |
| --- | --- |
| Преимущества | Возможные риски |
| * Облегчает проведение сложных расчетов. * Увеличивает скорость обработки информации. * Позволяет проводить дополнительные аналитические процедуры над имеющимися данными. * Увеличивает уровень безопасности данных посредством использования электронных средств защиты. | * Использование неточных данных. * Неправильное использование данных. * Проблемы безопасности (несанкционированный доступ к данным, несанкционированные изменения в исходных данных, пр.). * Невозможность своевременного обновления программного и/или аппаратного обеспечения.   Возможность утери данных. |

Аудит ИС позволяет оценить указанные риски и их последствия путем проверки логического и физического доступа к информационным ресурсам. Являясь одним из элементов оценки функционирования внутренней системы контроля компании, аудит ИС становится гарантом качества аудиторской проверки, т.к. позволяет оценить не только сами показатели финансовой деятельности предприятия, но и дать характеристику надежности процессу их формирования.

При этом у владельцев информационных систем возникает множество вопросов о роли информационной системы в стратегическом плане развития организации, вопросы оптимизации инвестиций в информационную систему. Кроме того, актуальны проблемы выявления и локализации проблем при сбоях в работе информационной системы, а также вопросы безопасности и контроля доступа. Также остаются актуальными вопросы оценки подрядных организаций при выполнении работ по настройке и поддержке информационных систем, а также необходимость в модернизации существующего оборудования и ПО. Руководитель организации и начальник Департамента автоматизации должны иметь возможность получать достоверную информацию о текущем состоянии информационной системы в кратчайшие сроки, иметь информацию о том, почему производится закупка дополнительного оборудования. Кроме того, немаловажным остается вопрос наличия рисков при размещении конфиденциальной информации в информационной системе организации, а также минимизации этих рисков. На подобные вопросы нельзя мгновенно дать однозначный ответ. Только рассматривая все взаимосвязи внутри информационной системы, учитывая нюансы и недостатки, можно получить достоверную и обоснованную информацию.

Программное обеспечение современного финансового учета позволяет вести учет одной и той же операции сразу в двух (или более) планах счетов. Преимущество таких программ заключается в том, что большая часть операций не требует двойной обработки документов. Таким образом, одна и та же операция может быть отражена в российском учете в рублях, а в «западном» в той валюте, которая определена учетной политикой предприятия.

К такому программному обеспечению относятся западные разработки (SCALA, SUN, АХАРТА и др.) и российские программы (1С, Контур, GAAP и др.). Несомненно, такие программы имеют ряд преимуществ: уменьшают затраты на формирование отчетности, позволяют формировать отчетность на двух языках, с такой программой могут работать как русскоязычные специалисты, так и не владеющие русским языком иностранные специалисты. Российские продукты рынка программного обеспечения предпочтительнее, т.к. отражают специфику российской бизнес - практики.

В подходе к тестированию функционирования ИС аудитор может использовать разные способы тестирования, а именно: инспектирование, наблюдение, запрос, подтверждение, сквозное тестирование.

Список литературы

1. Клочков M. Аудит сетевой и телекоммуникационной инфраструктуры // «Jetinfo» - M., 2015. - №4 (ресурс [www.jetinfo.ru](http://www.jetinfo.ru)).

2. Скабцов Н. Аудит безопасности информационных систем СП-б: Питер, 2018, 272 с.

References

1. Klochkov M. Audit of network and telecommunication infrastructure // Jetinfo - M., 2015. - No. 4 (resource www.jetinfo.ru).

2. Skabtsov N. Security Audit of Information Systems SP-b: Peter, 2018, 272 p.