

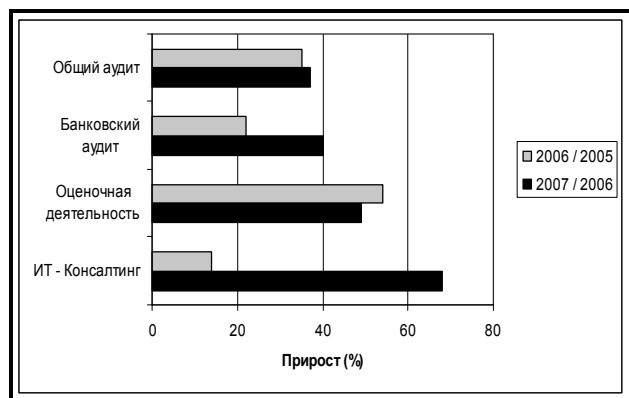
## 4.5. МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К АУДИТУ ИНФОРМАЦИОННЫХ СИСТЕМ

Баранова О.В., аспирант кафедры «Экономический анализ и аудит»

Финансовая академия при Правительстве РФ

В статье обозначены актуальные проблемы аудита информационных систем в среде компьютерной обработки данных, раскрыты основные подходы к аудиту информационных систем как составного элемента системы внутреннего контроля на предприятии и как самостоятельного объекта проверки. В статье рассматриваются текущие методики проведения аудита информационных систем, проводится их анализ через сравнение со стандартом CobiT, раскрываются основные элементы таких методических рекомендаций, как COSO, ITIL, CMMI.

В настоящее время аудит рассматривается предприятиями и пользователями бухгалтерской отчетности не только как функция проверки достоверности отчетности, но и как консалтинг в области управления рисками, анализа финансовой устойчивости, налогового консультирования, анализа систем внутреннего контроля и т.д. Одним из видов услуг, предлагаемых аудиторскими фирмами, является консультирование в области информационных технологий (рис. 1) [18].



**Рис. 1. Динамика роста выручки от аудиторско-консалтинговых услуг за 2006-й и 2007 гг. (в % к предыдущему году)**

Использование компьютерных данных бухгалтерского учета проверяемого экономического субъекта (ЭС) существенно повышает качество аудиторской проверки. С одной стороны, аудитор должен проверить влияние информационных систем (ИС) проверяемого предприятия на составление бухгалтерской отчетности, с другой стороны, аудитор не может проводить проверку и обработку больших массивов данных без использования вычислительной техники и программного обеспечения. Компьютеризированные процедуры аудита позволяют исследовать систему бухгалтерского учета аудируемого лица, ее организацию, отметить сегменты учета, требующие особого внимания аудитора.

Актуальность исследований в области теоретико-методологического аппарата аудита ИС обусловлена наличием проблемной ситуации, которая заключается, с одной стороны, в значительном влиянии информационных систем на составление бухгалтерской отчетности, а с другой – отсутствием методических рекоменда-

ций по проверке аудитором ИС и документированию проделанной работы.

Информационные технологии позволяют обрабатывать большие массивы информации, делая методологическую базу аудита наиболее полной и отвечающей современным требованиям аудиторского сообщества, однако использование аудитором программных продуктов для проведения проверки зачастую не находит отражения в рабочей документации, что в свою очередь обусловлено недостатком методических рекомендаций и (или) внутренних регламентов аудиторской фирмы.

Качество аудита зависит от ряда факторов, которые условно можно выделить в следующие группы.

- Качество информации, предоставляемой для аудита, включает следующие факторы:
  - профессиональные знания и навыки бухгалтеров проверяемого предприятия;
  - аудит информационной системы проверяемого экономического субъекта;
  - уровень понимания аудиторских процедур управляющим звеном аудируемого лица.
- Информационная прозрачность среды, в которой функционирует хозяйствующий субъект.

Таким образом, аудит информационных систем является одним из факторов обеспечения качества аудита.

Информационная система представляет собой совокупность программного и аппаратного обеспечения, используемого специалистами проверяемого экономического субъекта для обработки, хранения, трансформации и передачи финансовой информации. Таким образом, информационная система подразумевает наличие широкого спектра различных элементов.

Информационная система в более узком понимании может быть рассмотрена как конкретное программное и аппаратное обеспечение, используемое аудируемым лицом. К такому программному обеспечению можно отнести бухгалтерские ИС: «1С: бухгалтерия», «Парус», «Инфо-Бухгалтер» и др. Программное обеспечение может быть использовано для разных целей, а значит, аудируемое лицо может использовать несколько разных ИС. Таким образом, компьютерная обработка данных включает в себя обработку информации в ИС аудируемого субъекта.

Методология аудита ИС ставит своей задачей достижение разумного уровня уверенности в эффективности функционирования ИС в отношении следующих показателей ее работы (табл. 1).

Использование информационных технологий и, в частности, компьютерной техники в значительной степени оказывает влияние на оценку аудитором уровня риска и эффективности функционирования системы внутреннего контроля (СВК). Таким образом, главной задачей при проведении аудита в среде компьютерной обработки данных (КОД) является решение вопроса достоверности предоставленной информации.

Риски, связанные с обработкой данных в компьютерной и информационной системах аудируемого лица, можно разделить на две группы в зависимости от уровня их влияния:

- риски, оказывающие влияние на подготовленную финансовую отчетность;
- риски, влияющие на исходные финансовые данные, используемые для составления бухгалтерских отчетов.

Риски на уровне финансовой отчетности носят глобальный характер и влияют на поведение фирмы как в долгосрочном, так и краткосрочном периодах. В зависимости от уровня использования ИС их влияние на хозяйственную деятельность может быть измерено

различными показателями и соответствующими им рисками операционной деятельности (табл. 2).

Таблица 1

**ПОКАЗАТЕЛИ РАБОТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ**

Проверка эффективности следующих методологических основ функционирования ИС	<b>Разумная степень уверенности достигается в отношении</b>
Принципов функционирования	Нерушимости и отсутствия разрывов в многообразии связей между структурными компонентами АИС; состава элементов АИС и их полной гармонизации их между собой; гибкости и адаптивности ИС к внешним воздействиям; совместимости выбранной для обработки финансовой информации ИС с другими ИС, используемыми экономическим субъектом для эффективного функционирования; компонентов ИС с точки зрения их уникальности и сложности функционирования
Методов функционирования	Административных решений в части обязательного исполнения законов, директив, приказов и аналогичных регламентов, направленных на использование ИС в бизнес-процессах экономического субъекта; экономических и социально-идеологических решений в части материальной и социальной стимуляции сотрудников, направленной на эксплуатацию и улучшение действующих характеристик ИС
Способов функционирования	Соответствия дискрептивной модели, содержащейся в технической документации, ее реальным (фактическим) показателям функционирования; эффективности работы аппаратного обеспечения ИС

Таблица 2

**РИСКИ НА УРОВНЕ ФИНАНСОВОЙ ОТЧЕТНОСТИ**

Уровень использования ИС	Показатели	Риск
Вся фирма в целом	Полезность всей ИС; стоимость установки в расчете на одну рабочую станцию	Снижение эффективности работы всего предприятия вследствие неправильного выбора ИС; эффект от установки ИС на каждую рабочую станцию ниже, чем затраты по установке (неоптимальное соотношение в уравнении «затраты – качество»)
Отделы и департаменты производственного назначения	Объем продаж; качество продукта; ускорение процессов по выходу новых товаров на рынок	Снижение объема продаж вследствие увеличения себестоимости предлагаемых товаров; потеря места в ценовом сегменте рынка
Финансово-аналитические отделы	Изменение выручки; фондоотдача; различные показатели в расчете на одного сотрудника (напр., выручка в расчете на одного сотрудника)	Искажения и потери данных; искажение представления о фактическом положении экономического субъекта

Таким образом, среди показателей, характеризующих деятельность экономического субъекта, можно выделить следующие:

- экономичность (абсолютную или относительную экономию финансовых средств исходя из достигнутых количественных и качественных результатов использования ИС) – риски, связанные с чрезмерной экономией и недостаточным развитием ИС;
- результативность (степень достижения запланированных результатов и конечный социально-экономический эффект, полученный от использования ИС) – риск завышенных оценок и недостижимых целей;
- продуктивность (степень соотношения между полученными результатами и использованными на их достижение финансовыми, материальными и трудовыми ресурсами) – риски, связанные с уравнением затраты – качество.

Риски, влияющие на исходные бухгалтерские данные, также можно разделить на две крупные группы в соответствии с правилом (стандартом) «Оценка риска и внутренний контроль. Характеристика и учет среды компьютерной и информационной систем» (табл. 3):

- риски, связанные с концентрацией функций управления;
- риски, связанные с концентрацией данных и программ для их обработки.

Таблица 3

**РИСКИ, СВЯЗАННЫЕ С ИСХОДНЫМИ ДАННЫМИ**

Риски, связанные с концентрацией функций управления	Риски, связанные с концентрацией данных и программ для их обработки
Потеря разделения обязанностей, необходимой для эффективной работы ИС; риск проведения бухгалтерских записей без авторизации (визирования) расходов; риск несанкционированного доступа; риск несанкционированных бухгалтерских записей	Риск потери и (или) искажения данных вследствие утраты или порчи компьютеров, программного обеспечения; риск потери первичных документов; риски, связанные с осуществлением автоматических бухгалтерских записей; риски, связанные с формированием финансовой отчетности ИС в автоматическом режиме

В основе другой классификации рисков, связанных с проведением аудита экономического субъекта, работающего в среде КОД, лежат источники потенциальных опасностей. В данном случае выделяют следующие риски:

- риски, связанные с аппаратным и программным обеспечением проверяемого экономического субъекта;
- риски, связанные с квалификацией персонала;
- риски, связанные с отсутствием мер по обеспечению сохранности программ и данных компьютерного учета;
- риски, связанные с отсутствием контроля ввода исходных данных;
- риски, связанные с защитой и сохранностью финансовой информации.

В международной практике среди элементов СВК в среде КОД выделяют следующие:

- контрольная среда;
- оценка риска;
- контрольные процедуры;
- информация и коммуникация;
- мониторинг.

Контрольная среда является основой эффективной работы СВК, устанавливает стиль поведения в компании и охватывает проблемы в среде контроля, которые распространяются на всю организационную структуру предприятия.

Оценка риска требует со стороны руководства фирмы определения и анализа существующих рисков, их

релевантности к достижению поставленных в области контроля задач. Оценка риска является основой для формирования контрольных процедур.

Оценка риска может быть проведена на уровне самого экономического субъекта (для всей организации) или в отношении отдельной процедуры (отдельного бизнес-процесса или бизнес-единицы).

На уровне организации необходима оценка рисков соответствия требованиям законодательства (например, акт Сарбанеса-Оксли): руководство должно осуществлять необходимый контроль за разработкой стратегического плана развития информационных технологий предприятия, его своевременным и эффективным внедрением, общим соответствием требованиям различных регламентов.

Руководство также должно проводить оценку рисков в среде КОД, например, безопасность данных, изменений в используемых программах, др.

На уровне отдельной процедуры можно проводить:

- оценку риска на всех стадиях методологии функционирования ИС в среде КОД;
- оценку рисков неизбежных от функционирования ИС в среде КОД, а также вызванных сменой компонентов или самой ИС.

Контрольные процедуры представляют собой внутренние регламенты, процедуры и практические действия для достижения ЭС поставленных стратегических задач посредством снижения и (или) устранения рисков. Контрольные процедуры разрабатываются непосредственно для каждой рискованной ситуации, определенной руководством и описанной в контрольной среде.

Без надежно функционирующих в среде КОД ИС и контрольных процедур, поддерживающих это состояние, предприятия не смогли бы составлять достоверные отчеты. В практике аудита выделяются общие контрольные процедуры и прикладные. Общие контрольные процедуры созданы таким образом, чтобы отчеты, формируемые ИС, были достоверными. Прикладные контрольные процедуры встроены непосредственно в элементы ИС в среде КОД, чтобы предотвратить их неправильную работу.

Возрастающие объемы информации становятся все более сложными в управлении. Информация (содержание данных для достижения заданной цели) и коммуникация (средства их передачи до пользователей в нужной форме и в свое время) – важные составляющие СВК в среде компьютерной обработки данных.

Качество передаваемой информации зависит от ряда факторов:

- ее необходимости и релевантности;
- своевременности передачи;
- точности и достоверности данных;
- возможности доступа к данным пользователям.

Мониторинг представляет собой общий обзор всей СВК посредством продолжительной и временами одномоментной (разовой) оценки работы всех элементов СВК в компьютерной среде обработки данных. Выделяют два вида мониторинговых процедур: продолжительная оценка и одномоментные оценочные мероприятия.

Для понимания процессов аудита ИС в аудите необходимо использовать два подхода: попроцессный и поэлементный.

Суть попроцессного подхода заключается в проверке всех существенно важных процессов обработки финансовой информации в ИС, начиная со сбора информации и заканчивая предоставлением ее управляющему звену предприятия для анализа и формирования

управленческих решений. Попроцессный подход включает ряд этапов:

- 1-й этап – моделирование процессов;
- 2-й этап – декомпозиция модулей;
- 3-й этап – анализ.

Попроцессный подход предполагает индуктивное движение мысли исследователя, т.е., например, сложный процесс учета основных средств (ОС) разбивается на ряд модулей, которые в дальнейшем могут подвергнуться более детальному дроблению:

- учет покупки и постановки на учет объектов ОС;
- учет амортизации ОС;
- учет реконструкции и модернизации;
- учет выбытия объектов ОС.

При поэлементном подходе аудитор достигает разумную уверенность в отношении элементов функционирования ИС в части обеспечения достоверности финансовой отчетности экономического субъекта. Под элементами в данном случае понимаются структурные единицы ИС. Например, к элементам бухгалтерской ИС «1С: Бухгалтерия» можно отнести основные свойства плана счетов, виды аналитического учета, состав и структура используемых справочников, документов и журналов, констант.

Поэлементный подход к аудиту ИС подразумевает разделение структурных компонентов (элементов) хозяйственных операций в ИС и проверку их работы. Структурные элементы делятся на две группы: функциональные и информационные.

Функциональные элементы в свою очередь подразделяются на модули технического, технологического и эргономического обеспечения, при аудите которых аудитору следует рассмотреть возможности привлечения внешних экспертов.

Проанализировав теоретические основы проведения аудита в условиях КОД и оценки риска и внутреннего контроля в среде компьютерной и информационной систем аудируемого субъекта, необходимо объединить фундаментальные положения аудита в виде методических рекомендаций по проведению проверки в среде КОД ЭС.

Методика аудита в условиях КОД и оценки риска и внутреннего контроля должна повысить качество аудиторских услуг посредством реализации следующих задач:

- объединение общих теоретических основ аудита в виде практического инструмента проверки эффективности работы СВК аудируемого лица в среде компьютерной обработки данных;
- предоставление эффективного метода расчета и оценки риска внутреннего контроля в среде КОД;
- повышение скорости работы аудитора в результате использования универсальной методики проверки среды КОД ЭС, формально закрепленной внутренними регламентами аудиторской фирмы;
- предоставление инструмента в формировании выводов относительно функционирования ИС аудируемого лица.

Основные положения методики должны отражать три ключевых аспекта аудита в среде КОД – работа аудитора в среде КОД ЭС, оценка СВК аудируемого субъекта и оценка риска в среде КОД.

Практически реализовать поставленную цель можно посредством ряда процедур, а именно, наблюдения, инспектирования и опроса.

Наблюдение – наиболее простой из предложенных способов, поскольку не требует особых навыков. Однако данный способ можно использовать в отношении документирования ограниченного числа элементов среды КОД. Например, уровни доступа не могут быть

всесторонне изучены только посредством наблюдения за сотрудниками фирмы.

Инспектирование документации – способ, требующий от аудитора определенных навыков, поскольку подразумевает не только механический перенос данных с одного документа в другой (рабочая документация аудитора), но и оценку релевантности регламентов, установленных в организационной структуре проверяемого субъекта. Например, аудитор имеет возможность оценить частоту и эффективность контрольных проверок, полноту и существенность предоставляемых по результатам проверок отчетов, адекватность мер, принимаемых по результатам проверок.

Опрос может быть проведен как среди высшего руководства, так и среди рядовых сотрудников проверяемого предприятия. Опрос позволяет получить информацию в отношении тех областей оценки работы аудитора в среде компьютерной обработки данных, которые были не полностью или совсем не оценены в рамках предыдущих процедур.

Помимо указанных традиционных методов (инспектирование документации, устный и письменный опрос) аудитор может прибегнуть к такому методу как метод концептуальных связей.

Используя метод концептуальных связей (concept mapping), аудитор может наглядно представить взаимосвязь между элементами среды КОД. Метод концептуальных связей представляет собой способ определения очевидных закономерностей между событиями и объектами или отображениями в среде КОД событий и объектов, объединенных общим назначением. Под концепцией в целях проведения проверки подразумеваются понятия, характеризующие функционирование среды КОД.

Метод концептуальных связей разработан на основе теории Д. Аусубела об эффективном обучении, которая утверждает, что эффективное обучение – это процесс, в котором новая информация сопоставляется с существующим аспектом в человеческой структуре знания [22].

Метод концептуальных связей способствует движению необходимой информации путем определения и отображения связей между полученной на стадии планирования информацией и ожидаемых данных. Наиболее наглядной реализацией данного метода на практике является построение графических моделей. На начальном этапе построения графической модели она может представлять собой вертикальную иерархию из блоков информации под общими условными названиями или разрозненные данные о работе ЭС в среде КОД. При более детальном изучении и выявлении глубинных процессов в каждом из блоков информации графическая модель пополняется горизонтальными связями. На этой стадии необходимо провести правильное сопоставление предварительных данных с полученными в ходе описания среды КОД (рис. 2).

Уровень детализации концептуальных связей зависит от поставленной задачи и практических возможностей ее реализации, например, отсутствие доступа к внутренним регламентам ЭС (технической документации) может привести к тому, что аудитор не получит всестороннего понимания уровня предоставления доступа к различной информации в среде КОД, что может привести к увеличению масштаба аудиторских процедур в ходе осуществления проверки.

Применение метода концептуальных связей позволяет путем дедукции получить необходимую глубину понимания процессов в среде КОД ЭС.

В ходе описания среды КОД аудитор также может прибегать к методу ранжирования. Ранжирование подразумевает распределение приоритетов. Например, в зависимости от масштаба бизнеса автоматизация работы отдела расчета заработной платы может быть разной, поэтому в ходе работы аудитор должен оценить важность данного элемента среды КОД и необходимость его детального изучения.

Ранжирование позволяет аудитору делать акцент в своей работе на наиболее значимые элементы среды КОД, уделять им больше времени для изучения и оценивать важность привлечения экспертов.

Распределяя приоритеты работы в описании среды КОД, аудитор снижает риск необнаружения. Риск необнаружения выражает вероятность того, что выполнение всех аудиторских процедур и соответствующий сбор доказательств не позволят обнаружить ошибки, превышающие допустимую величину [6].

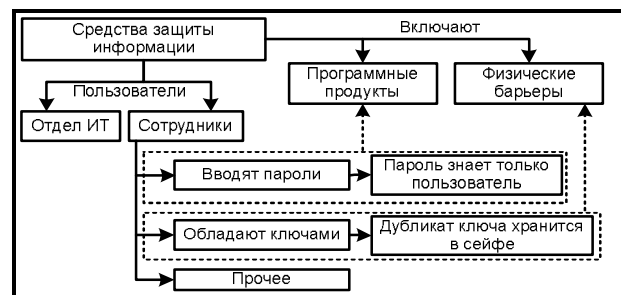


Рис. 2. Метод концептуальных связей

Независимо от способа, выбранного для проверки работы ИС и баз данных – по процессный или поэтапный, аудитор выделяет следующие группы:

- методы изучения и анализа фактического состояния ИС предприятия;
- методы графического представления фактического состояния ИС предприятия.

К методам изучения и анализа фактического состояния ИС ЭС можно отнести следующие:

- устный и письменный опрос;
- письменное анкетирование;
- наблюдение;
- измерение и оценка.

После предварительного сбора и изучения информации относительно различных элементов и (или) процессов ИС и баз данных члены аудиторской команды могут применить такой метод, как групповое обсуждение для выявления областей потенциального риска и их влияния на финансовую отчетность предприятия и непосредственно аудиторские процедуры по проверке финансовой отчетности.

Более того, аудиторы в ходе группового обсуждения прибегают к методу анализ задач, суть которого состоит в вертикальной и горизонтальной структуризации задач и их распределения между членами аудиторской команды.

Следующий метод – анализ информационных процессов. Анализ информационных процессов – сложный многогранный метод, который включает следующие более конкретные аналитические процедуры:

- моделирование информационного процесса;
- структурное (модульное) проектирование;
- декомпозиция модулей;
- анализ модулей информационного процесса;
- анализ эффективности.

При анализе по степени влияния на финансовую отчетность модули ИС делятся на модули прямого и косвенного воздействия, а также модули со значительным и слабым влиянием. Следует отметить, что не существует модулей ИС, которые бы не оказывали на финансовую отчетность никакого влияния, так как последняя является отображением состояния дел на предприятии и аккумулирует в себе все данные о хозяйственной деятельности.

При выборе модулей для анализа с использованием степени их влияния аудитор учитывает уровень существенности и временные затраты, особенно если модуль косвенно воздействует на финансовую отчетность. Элементы ИС с прямым воздействием могут иметь как значительное, так и слабое влияние на финансовую отчетность, то же справедливо и про элементы косвенного воздействия.

Важными относительными показателями работы информационной системы является наличие приборов фиксаторов в разных точках контроля, позволяющих зафиксировать следующие показатели:

- среднее время выполнения процесса за период;
- средняя стоимость процесса за период;
- число прерванных процессов;
- число завершенных процессов;
- число процессов, выполненных с задержкой.

Точки контроля на практике часто располагаются на стыке различных подразделений, взаимодействующие в рамках одного процесса, выполнение которого протекает в ИС. Точки контроля позволяют аудитору сузить области поиска отклонений в ходе анализа.

Применение эвристических методов анализа возможно в случае, когда аудитор сталкивается с нехваткой информации или проблемой в анализе, которая требует значительных знаний.

Среди многочисленных эвристических методов анализа предлагается использовать метод аналогий, методы опроса, или контрольных вопросов, анкетирование и интервьюирование, метод контрольных вопросов и метод «мозгового штурма».

Метод аналогий основывается на прошлом опыте экспертов в анализе аналогичных элементов ИС. В этом случае большую ценность представляют материалы с описанием аналогичных информационных систем, а также знания экспертов.

Метод опроса, или контрольных вопросов, использует знания экспертов, аккумулируя и структурируя их в виде тщательно подготовленных вопросников по заданной теме. В этом случае аудитор может использовать свободный или формализованный вопросник. Свободный формат предполагает развернутые ответы экспертов и наиболее сложен при анализе. Формализованный вопросник предлагает экспертам варианты ответов.

Метод анкетирования похож на метод опроса, он также проводится по средством анкеты, в которой:

- формулировки должны исключать смысловую неопределенность;
- должны быть использованы общепринятые термины;
- обеспечено единое и однозначное толкование результатов анкетирования [2].

Интервьюирование в свою очередь предполагает межличностное общение, т.е. диалог между респондентом и интервьюером. Положительной стороной данного метода является возможность модификации заданных вопросов в ходе беседы.

Метод контрольных вопросов основывается на использовании анкет табличной формы с вопросами и

заранее проставленными ответами. Задача эксперта состоит в том, чтобы выбрать наиболее подходящий, по его мнению, вариант ответа. Вопросы при таком анализе являются параметрами оценки объекта, а ответы – значениями параметров.

В ходе анализа работы модуля ИС аудитор может столкнуться с проблемой, которая до этого не встречалась в его практике, и традиционные аналитические методики не дают возможности определить источники проблемой ситуации. В этом случае аудитор может прибегнуть к такому способу, как «мозговой штурм», т.е. эксперты аудиторской фирмы (или, если необходимо, то и внешние эксперты), хорошо знающие сложившуюся ситуацию, собираются для того, чтобы провести свободное генерирование идей по поиску решения в сложившейся ситуации.

В международной практике для анализа информационных систем аудиторы используют рекомендации ряда методических пособий (стандартов), которые в большинстве своем больше отвечают интересами сотрудников технических специальностей, нежели интересам аудиторской проверки. К таким методическим пособиям относят **Cobit**, **COSO**, **ITIL**, **CMMI** и пр.

**Cobit** – это собрание лучших практических рекомендаций в области управления, контроля и проверки ИТ. Целью данного методического руководства является исследование, разработка и распространение современных и глобально приемлемых правил в сфере управления ИТ и их проверки.

Данный стандарт охватывает широкий спектр вопросов качественной проверки информационных технологий и, в частности, ИС. Для аудиторов положительной чертой практических рекомендаций, собранных в рамках данного стандарта, является описательный характер и отсутствие узко специальных технических терминов. **Cobit** рассматривает управление ИТ и проверку их работы как процессы, связанные с общей стратегией управления бизнесом, т.е. неэффективное управление в области ИТ может привести к низким результатам в бизнесе, и наоборот. В рамках стандарта реализуется подход **PDCA**-цикла (PDCA: plan – do – check – act, то есть планируй – делай – проверяй – действуй). Требования бизнеса должны соответствовать возможностям информационных технологий, а также должны быть четко задокументированы и количественно и качественно измерены (plan, т.е. планируй). Выбранное решение должно быть внедрено и использовано (do т.е. делай). Результаты от внедрения должны соответствовать критериям, выбранным на первом этапе (check, т.е. проверяй). Отклонения должны быть оценены и необходимые меры приняты (act, т.е. действуй).

**COSO** – стандарт, призванный улучшить качество финансовой отчетности через эффективное управление системой внутреннего контроля. Данный стандарт был опубликован в 1992 г. Комитетом спонсорских организаций (Committee of sponsoring organisations).

Стандарт состоит из четырех частей:

- «Введение» (Executive summary) представляет собой обзор общего подхода к внутреннему контролю;
- «Подход» (Framework) дает определение СВК, ее компонентов и содержит критерии оценки СВК предприятия;
- «Отчеты перед внешними пользователями» (Reporting to external parties) – часть стандарта, которая дает общие рекомендации по составлению отчетов о функционировании СВК как для составителей и менеджмента фирмы, так и для внешних пользователей;

- «Способы оценки» (Evaluation tools) содержит практические рекомендации, полезные при проведении внутренней оценки СВК.

«Подход» – это основная часть в данном стандарте, она содержит описание общих методических и частных практических вопросов функционирования СВК. Внутренняя контрольная процедура в **COSO** определяется как процесс, подвергаемый влиянию совета директоров, руководства и другого персонала предприятия, разработанный с целью предоставления разумной уверенности в отношении достижения поставленных целей в следующих областях:

- эффективность и производительность операционной деятельности;
- надежность финансовой отчетности;
- соблюдение необходимых законов и регламентов [20].

Таким образом, как следует из определения, данный стандарт предполагает разделение всех задач предприятия на три группы – операционная деятельность, финансовая отчетность, соответствие законодательным актам. Достижение поставленных целей осуществляется посредством реализации руководством предприятия последовательных действий в следующих областях (описанных выше в тексте статьи):

- контрольная среда;
- оценка риска;
- контрольные процедуры;
- информация и коммуникация;
- мониторинг.

**ITIL** (IT infrastructure library) представляет собой серию книг, в которых изложены теоретические аспекты и практический опыт в области управления ИТ и предоставления высококачественных информационных услуг. В настоящее время действительными являются публикации второй версии стандарта, которые включают восемь книг:

- управление программным обеспечением (software asset management);
- сервисная поддержка (service support);
- доставка сервисов (service delivery);
- планирование внедрения управления сервисом (planning to implement service management);
- управление инфраструктурой **ICT** (ICT infrastructure management);
- управление прикладными программами (application management);
- управление безопасностью (security management);
- бизнес-перспективы, часть 2 (business perspective, volume II).

В 2007 г. появилась новая третья версия библиотеки лучшего опыта в сфере управления сервисами **ITIL**. Новая версия состоит из трех частей:

- ядро (core);
- дополнительные книги (complementary);
- Интернет-часть (Web).

В «ядро» входят следующие книги:

- по сервисной стратегии (service strategy);
- по переходным процессам сервисов (service transition);
- по операционным процессам сервисов (service operation);
- по проектированию сервисов (service design) и их постоянному совершенствованию (continual service improvement) [12].

Серия дополнительных книг (complementary) должна стать наглядным руководством для действий работников сферы ИТ, учитывая отдельные секторы рынка (государственный, финансовый, пр.) и национальные особенности (например, практика управления сервисами в Японии отличается от европейской), и ответить на вопрос «как сделать?».

Тем не менее, **ITIL** может быть полезен аудиторам, так как предоставляет две концепции работы информационных технологий: целостный подход к управлению сервисом и ориентация на пользователя. Целостный подход к управлению

сервисом рассматривает процесс управления в целом, а не его отдельные части, и учитывает, что:

- все требования к операционной деятельности и поддержке учитываются;
- разрабатываются планы тестирования;
- определяется влияние измененной или новой ИС на существующую инфраструктуру;
- определяются будущие требования.

Ориентация на пользователя является основой надежного функционирования в будущем. Для обеспечения качества такого уровня следует разделять ответственность между сотрудниками, которые:

- консультируют пользователей и помогают им оптимально использовать доступные ресурсы;
- собирают и обрабатывают мнения пользователей и их жалобы;
- отслеживают жалобы;
- проводят мониторинг оценок пользователей сервисов;
- осуществляют поддержку внутренних групп пользователей.

Аудитор также может следовать целостному подходу только не к управлению, а к проверке ИС и их влияния на финансовую отчетность. Целостность заключается в разработке универсальных программ аудита, готовых к использованию и учитывающих требования всех сторон – пользователей услуг и аудиторов. Определение и прогнозы эффектов влияния новых и модифицированных систем также оказывает помощь аудитору в оценке влияний информационных компонентов на финансовую отчетность.

**CMMI** (capability maturity model integration) – это собрание практических рекомендаций для улучшения процессов разработки программных продуктов, ИС. Стандарт был издан американским институтом Software engineering institute (SEI) в 2002 г.

Данный стандарт покрывает четыре предметные области, которые в самом стандарте называются дисциплинами:

- системный инжиниринг (system engineering);
- инжиниринг программного обеспечения (software engineering);
- разработка встроенных продуктов и процессов (integrated product and process development, IPPD);
- работа с поставщиками (supplier sourcing).

Системный инжиниринг рассматривает процессы разработки систем, иногда включая программное обеспечение. Эта дисциплина сфокусирована на основных потребностях финальных пользователей, их ожиданиях от информационной системы и ограничениях, которые могут помешать ее оптимальному функционированию.

Программный инжиниринг рассматривает процессы разработки, в т.ч. применение систематического подхода с количественными аспектами к разработке, функционированию и его поддержке.

Разработка встроенных продуктов и процессов – это подход, который обеспечивает своевременное взаимодействие пользователей с разработчиками на протяжении всего процесса разработки и функционирования информационной системы.

Работа с поставщиками – это дисциплина, которая рассматривает приобретение дополнительных продуктов от поставщика, т.е. возможные функции поддержки, обновления компонентов систем, добавления новых модификаций.

Наиболее продуктивным считается рассмотрение всех четырех дисциплин пользователем одновременно, особенно первых двух.

В ходе анализа системы с применением **CMMI** выделяются уровни возможностей и зрелости. Уровень возможностей (capability level) рассматривает общие и частные цели и практические действия по их реализации. Существует шесть уровней возможностей:

- уровень 0 – незаконченный;
- уровень 1 – работающий / текущий;

- уровень 2 – управляемый;
- уровень 3 – определенный и управляемый;
- уровень 4 – качественное управление;
- уровень 5 – оптимальный.

Уровни зрелости характеризуют предприятие в целом. Выделяют пять уровней, которые применяют к анализу каждой из областей процессов, рассмотренных выше:

- уровень 1 – начальный;
- уровень 2 – управляемый;
- уровень 3 – определенный;
- уровень 4 – управление качеством;
- уровень 5 – оптимальный.

Компоненты стандарта **СММИ** представлены в виде схемы на рис. 3.

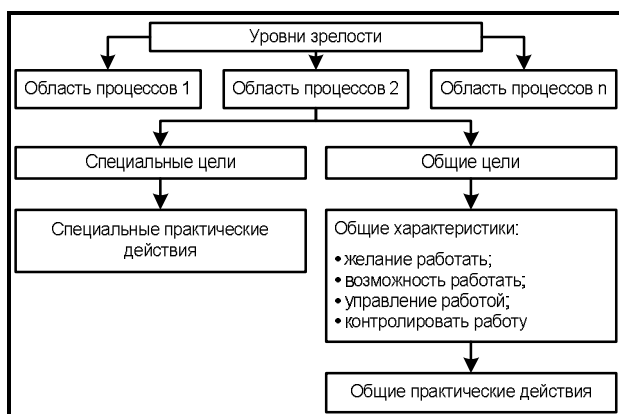


Рис. 3. Структурные компоненты стандарта **СММИ**

Область процессов включает:

- управление процессом состоит в том, чтобы эффективно определять, планировать, обеспечивать ресурсную базу, применять, проводить мониторинг, контролировать, измерять и оценивать, улучшать процессы в разных проектах. Иначе говоря, эта область стандарта ставит своей целью обеспечение максимальных выгод от обучения, инноваций и структурирования текущей деятельности предприятия;
- управление проектом похоже в своей практической реализации на управление процессом, только объектом управления, контроля и планирования является проект и усложняется взаимодействием с поставщиками, его качественным и количественным анализом, а также управлением рисками и анализом совместимости проекта с текущей ИС;
- инжиниринг – разработка и поддержка во всех процессах, сопутствующих созданию ИС (включая системные и программный инжиниринг), и включает:
  - планирование проекта;
  - мониторинг и контроль проекта;
  - работу с поставщиками;
  - анализ совместимости проекта и управление рисками;
  - управление персоналом (командная игра);
- поддержка – это действия, которые сопровождают процесс разработки, в таких областях, как управление конфигурациями, менеджмент качества продукта, измерение и оценка, подготовка организационной структуры к внедрению, анализ решений, анализ случайных событий и методов решения их исходов.

Задача данного стандарта – в сокращении издержек и затрат по улучшению текущей ИС посредством логического и последовательного анализа текущих процессов ее управления.

Рассмотрев основные стандарты, используемые в области управления и анализа ИС, целесообразно провести их сравнение с наиболее полным и детальным стандартом **CobIT** по процедурам, которые в нем рассмотрены, и в качестве категорий оценки выбрать частоту и глубину раскрытия информации (табл. 4).

Таблица 4

СРАВНИТЕЛЬНАЯ ТАБЛИЦА ДЛЯ СТАНДАРТОВ **COBIT, COSO, ITIL, СММИ**<sup>1</sup>

Группа	№	Процедуры в рамках стандарта <b>CobIT</b>	<b>COSO</b>	<b>ITIL</b>	<b>СММИ</b>
Планирование и организация	<b>PO1</b>	Определять стратегические задачи ИТ	+	-	-
	<b>PO2</b>	Определить информационную архитектуру	+	-	-
	<b>PO3</b>	Определить технологические направления	+	+	-
	<b>PO4</b>	Определить организационные аспекты	+	+	-
	<b>PO5</b>	Управление финансированием ИТ	+	+	-
	<b>PO6</b>	Цели управления коммуникациями и направления их развития	+	-	-
	<b>PO7</b>	Управление людскими ресурсами	+	-	-
	<b>PO8</b>	Согласование с внешними требованиями	-	-	+
	<b>PO9</b>	Оценка рисков	+	-	+
	<b>PO10</b>	Управление проектами	-	-	+
Приобретение и ввод в действие	<b>AI1</b>	Выбор решений и их документирование	+	-	-
	<b>AI2</b>	Приобретение и поддержка прикладного ПО	+	-	+
	<b>AI3</b>	Приобретение и поддержка технологического оборудования	+	-	-
	<b>AI4</b>	Разработка и поддержка процедур ИТ	+	+	-
	<b>AI5</b>	Установка и проверка систем	-	-	-
	<b>AI6</b>	Управление изменениями	+	+	+
	<b>AI7</b>	Установка решений и изменений	+	+	+
Доставка и поддержка	<b>DS1</b>	Определить требования к сервису	+	+	-
	<b>DS2</b>	Управление сервисом, предоставляемым внешними организациями	-	+	-
	<b>DS3</b>	Управление выполнением и качеством	+	+	-
	<b>DS4</b>	Гарантии доступности сервиса	+	+	-
	<b>DS5</b>	Гарантии безопасности	+	+	-
	<b>DS6</b>	Идентификация свойств и их ценности	-	+	-
	<b>DS7</b>	Обучение пользователей	+	-	+
	<b>DS8</b>	Помощь и советы пользователям ИТ	-	+	-
	<b>DS9</b>	Управление конфигурацией	+	+	+
	<b>DS10</b>	Управление инцидентами и проблемами	-	+	+
	<b>DS11</b>	Управление данными	+	+	+
	<b>DS12</b>	Управление средствами	+	-	-
	<b>DS13</b>	Управление операциями	-	-	-
Мониторинг	<b>M1</b>	Выделение процессов, за которыми необходимо наблюдать	-	-	+
	<b>M2</b>	Оценка адекватности внутреннего управления	-	-	-
	<b>M3</b>	Получение независимой оценки	+	-	-
	<b>M4</b>	Обеспечение независимого аудита	+	-	-

Рассмотрим другой аспект аудита информационных систем – использование самим аудитором информационных систем для работы с данными, предоставляемыми аудируемым лицом для проверки. Принимая во внимание растущий объем бухгалтерских и управленческих данных, их сложность и способы организации информации, аудит без использования информационных систем практически невозможен.

Для автоматизации аудита в настоящее время применяются различные программные средства, которые можно поделить на следующие группы:

- справочно-информационные системы («Ассистент аудитора»);
- системы автоматизации непосредственно процесса аудиторской проверки («ЭкспрессАудит: ПРОФ», «AuditXP» («Комплекс аудит»), «IT Audit: Аудитор»);
- системы, охватывающие всю деятельность аудиторской фирмы (AuditNET).

Эти программы нацелены на решение различных задач и удовлетворяют потребности различных целевых групп аудиторского сообщества. Выбор автоматизированной информационной системы аудита – это поиск оптимального соотношения функциональности предложенной сис-

<sup>1</sup> Примечание к табл 4: "+" полное раскрытие; "-" неполное раскрытие.

темы и затрат на ее внедрение, а также оценка уровня надежности фирмы-производителя [9].

По мнению автора, автоматизированные информационные системы аудита должны обязательно включать следующие элементы:

- модуль сопровождения аудита;
- модуль финансового анализа и аудиторских процедур;
- модуль справочно-правовой базы;
- модуль хранения информации.

Модуль сопровождения должен содержать все необходимые методические и методологические указания по проведению аудита, т.е.:

- все необходимые аспекты предварительного анализа аудируемого лица с указанием областей потенциального риска как для аудитора, так и для хозяйствующего субъекта (например, неэффективно построенные процедуры системы внутреннего контроля);
- общий план аудита, содержащий информацию об объеме и порядке проведения аудита;
- программы аудита, т.е. методики по проведению проверок (например, перечисление конкретных аудиторских процедур, необходимых для проверки предпосылки существования объектов основных средств), способы их реализации и временные рамки;
- в случае необходимости документ, позволяющий оценить риски операционной деятельности проверяемого хозяйствующего субъекта и их влияние на составления финансовой отчетности.

В данном разделе должны быть реализованы различные подходы к определению этапов (сегментов, разделов) аудита, а именно:

- пообъектный подход;
- деагрегация финансовой отчетности;
- циклический подход.

Наиболее простым и понятным аудитору способом, реализованным в существующих в настоящее время на рынке программных продуктах, является пообъектный подход. В данном подходе разделы проверки соответствуют объектам бухгалтерского учета – активам, обязательствам, доходам, расходам, капиталу.

При пообъектном подходе аудитор легко формулирует процедуры программы и полностью покрывает в ходе проверки объекты учета, которые отражаются в отчетности. Кроме того, получение информации в ходе проверки также облегчается, так как в основе организационной структуры большинства предприятий лежит та же классификация объектов, что и в бухгалтерском учете, например, отдел калькулирования себестоимости. Тем не менее, при своей простоте и понятности подход не лишен недостатков, одним из которых является многократное обращение членов аудиторской группы к одним и тем же источникам информации. Влияние указанного недостатка может быть снижено при правильной организации работы внутри группы аудиторов ее руководителем.

В случае деагрегации финансовой отчетности «каждая статья отчетности разлагается на составляющие вплоть до отдельных остатков или оборотов по счетам, ее формирование прослеживается вплоть до первичных документов и хозяйственных операций» [11].

Несмотря на высокую точность данного подхода к планированию аудита, он обладает существенным недостатком. В отличие от пообъектного подхода, при деагрегации финансовой отчетности существует возможность пропуска тех или иных разделов учета, групп существенных операций или остатков по счетам, напрямую не отраженных в отчетности.

Последний подход к планированию аудита – аудит по циклам финансово-хозяйственной деятельности. В этом случае объектом проверки служат обороты по счетам бухгалтерского учета, так как именно они отражают финансо-

во-хозяйственную деятельность предприятия в течение года, а не остатки по счетам. Данный подход наименее распространен в российской практике аудита, так как сложен для понимания аудиторами, которые с трудом выделяют циклы хозяйственной деятельности.

В своей статье «Подходы к формированию программы аудиторской проверки» к.э.н. Коменденко С.Н. предлагает следующую классификацию циклов:

- циклы основной (текущей) деятельности (цикл приобретение ресурсов, цикл использования ресурсов, цикл продаж, цикл расчетов по текущей деятельности);
- циклы инвестиционной деятельности (цикл приобретения активов, цикл использования активов, цикл ликвидации активов, цикл расчетов по инвестиционной деятельности);
- циклы финансовой деятельности (цикл привлечения капитала, цикл использования капитала, цикл возврата капитала) [11].

В случае выбора циклического подхода к аудиту каждый из циклов легко разбивается на однотипных, и далее аудит проводится в зависимости от уровня существенности. Таким образом, аудит циклов включает в себя циклы 1-го, 2-го и 3-го уровней. Например:

- цикл 1-го уровня – цикл приобретения ресурсов;
- цикл 2-го уровня – закупка материалов;
- цикл 3-го уровня – закупка по группам материалов.

Модуль финансового анализа и аудиторских процедур призван облегчать в процессе проведения аудиторской проверки расчет различных показателей финансового анализа, а также способствовать осуществлению аналитических тестов и тестов по существу.

Наличие модуля справочно-правовой базы облегчит работу аудиторов в части поиска законодательных и нормативно-правовых документов.

Модуль хранения информации – важная составляющая автоматизированной информационной системы аудита, которая обеспечивает не только возможность постоянного доступа к необходимым данным, но и, организованная на должном уровне, соблюдает принцип конфиденциальности, аудиторской тайны.

Специфика аудиторской работы состоит в том, что сотрудники фирмы часто уезжают в длительные командировки. Общение и обмен данными, обращения к серверу компании в таких условиях затруднены по ряду причин, одной из которых является безопасность данных.

Данная проблема может быть решена при обеспечении удаленного доступа. Однако находясь в недоверенной среде (вне офиса), аудитор сталкивается с необходимостью ввода пароля для собственной аутентификации на сервере аудиторской фирмы с чужого компьютера (например, компьютер бухгалтера аудируемого лица или компьютера в Интернет-кафе). Проблема состоит в том, что пароли сохраняются в кэш-памяти компьютера, а потому могут быть использованы другими пользователями.

Аппаратные устройства безопасного доступа, такие как смарт-карты и USB-ключи, являются решением проблемы. Помимо указанных средств, также существует концепция одноразовых паролей (ОП). ОП – это ключевое слово и (или) набор символов (цифр), действительные только для одного процесса аутентификации в течение ограниченного промежутка времени. Такой пароль полностью решает проблему возможного перехвата информации злоумышленниками.

В современных технологиях аутентификации с помощью ОП применяется динамическая генерация ключевых слов с помощью сильных криптографических алгоритмов, т.е. аутентификационные данные – это результат шифрования какого-либо начального значения с помощью секретного ключа пользователя. Данная информация есть у пользователя и у сервера. Она не передается по сети и недоступна для перехвата. В качестве начального значения используется известная обоим сторонам процесса аутентификации



информация, а ключ шифрования создается для каждого пользователя при его инициации в системе [19].

Программные средства аудита могут быть предназначены не только для проверки содержания компьютерных файлов аудируемого лица, но и для выполнения ряда непосредственно аудиторских процедур – тестов по существу, аналитических процедур, пр.

### Проверка компьютерных файлов аудируемого лица

ИС аудита может быть использована для прочтения (отображения) обрабатываемых данных, осуществления тестов по существу, а именно:

- проверка и анализ записей на основе критериев качества, полноты, состоятельности и правильности;
- тестирование выполнения расчетов;
- сопоставление данных различных файлов с целью выявления несопоставимых данных;
- доступ к данным с целью их упорядочивания, сортировки, группировки данных по различным признакам и автоматического формирования отчета по результатам теста [17].

### Аудиторские процедуры в АИС аудита

Программные продукты аудита также могут быть использованы для проведения ряда процедур, например:

- составление выборки в соответствии со статистическими методами по заданному критерию;
- проведение трендового анализа;
- расчет коэффициентов экономического анализа (оборачиваемость, рентабельность, фондоотдача, прочие);
- проведение анализа дебиторской задолженности по срокам возникновения; проведение анализа запасов, объектов готовой продукции по датам прихода на склад.

В условиях постоянно и динамично меняющегося общества роль аудита информационных систем в среде компьютерной обработки данных невозможно недооценить. Создание и быстрое развитие коммерческих структур различной организационно-правовой формы потребовало от рынка создания сложных информационных систем бухгалтерского учета, отвечающих требованиям усложняющихся бизнес-процессов, которые в свою очередь являются объектом проверки со стороны аудиторов. Поэтому практическая аудиторская деятельность невозможна без создания методических рекомендаций по проверке информационных систем предприятий в среде компьютерной обработки данных с применением информационных технологий.

### Литература

1. Автоматизированные информационные технологии в экономике [Текст] / под ред. проф. Г.А. Титоренко. – М. : ЮНИТИ, 2006.
2. Баканов М.И. Теория экономического анализа [Текст] / М.И. Баканов, М.В. Мельник, А.Д. Шеремет. – М. : Финансы и статистика, 2006.
3. Баранова О.В. Аудит информационных систем в условиях компьютерной обработки данных [Текст] / О.В. Баранова // Экономика и управление качеством: учет, анализ, методы, модели, инструменты и аудит : сб. науч. тр. – Тамбов : ТГТУ, 2008.
4. Баранова О.В. Информационные системы аудита [Текст] / О.В. Баранова // Финансовый бизнес. – 2006. – №2. – С. 53-58.
5. Баранова О.В. Методология аудита в среде компьютерной обработки данных [Текст] / О.В. Баранова. – М. : Компания Спутник+, 2008.
6. Бычкова С.М., Растамханова Л.Н. Риски в аудиторской деятельности [Текст] / С.М. Бычкова, Л.Н. Растамханова. – М. : Финансы и статистика, 2003.
7. Горемыкин А. Автоматизация аудита [Текст] / А. Горемыкин // Финансовая газета. – 2005. – №7.

8. Давлетханов М. Концепция одноразовых паролей в системе аутентификации [Текст] / М. Давлетханов // ВУТЕ/Россия. – 2006. – №7-8.
9. Еремин Л. Информационные технологии [Текст] / Л. Еремин // Финансовая газета. – 2005. – №27.
10. Исаев Г.Н. Информационные системы в экономике [Текст] / Г.Н. Исаев. – М. : Омега-Л, 2006.
11. Коменденко С.Н. Подходы к формированию программы аудиторской проверки [Текст] / С.Н. Коменденко // Аудитор. – 2006. – №1.
12. Лезезо Д. Третий пошел. ITIL v.3 [Текст] / Д. Лезезо // Intelligent enterprise. – 2008. – №2.
13. Патрушина С.М. Информационные системы в бухгалтерском учете [Текст] / С.М. Патрушина. – М. : ИКЦ «МарТ», 2003.
14. Подольский В.И. Компьютерный аудит [Текст] / В.И. Подольский, Н.С. Щербаклова, В.Л. Комиссаров. – М. : ЮНИТИ-ДАНА, 2004.
15. Сиротенко Э.А. Информационное моделирование аудиторской деятельности [Текст] / Э.А. Сиротенко. – М. : Финансовая академия при Правительстве РФ, Оргсервис-2000, 2004.
16. Сиротенко Э.А. Перспективы развития теоретико-методологического аппарата аудита [Текст] / Э.А. Сиротенко // Аудиторские ведомости. – 2006. – №1. – С. 17-24.
17. Федорова Г.В. Информационные технологии бухгалтерского учета, анализа и аудита [Текст] / Г.В. Федорова. – М. : Омега-Л, 2006.
18. Ханферян В.В. Рынок аудиторско-консалтинговых услуг в 2007 году [Электронный ресурс] / В.В. Ханферян // Энциклопедия Эксперт РА. 2008.
19. Book on IT Control Objectives for Sarbanes-Oxley. The Role of IT in the design and implementation of internal control over financial reporting, 2<sup>nd</sup> Edition. – USA: IT Governance Institute, 2006.
20. Cobit Mapping: Overview of International IT Guidance, 2<sup>nd</sup> edition. – USA, IT Governance Institute. – 2006.
21. IT Examination Handbook. Audit. – Federal Financial Institutions Examination Council, 2003.
22. Kristine M. Protzman, Vasant Raval. Concept Mapping – A learning tool for information systems audit profession. // Information systems control journal. Vol. 3. 2004.

### Ключевые слова

Внешний аудит; система внутреннего контроля; информационная система; аудиторские риски; компьютерная обработка данных; методология аудита; стандарт CobIT; риски бухгалтерской отчетности; программное обеспечение аудитора; оценка риска.

Баранова Ольга Владимировна

### РЕЦЕНЗИЯ

В современных условиях становление аудита и в целом аудиторской деятельности должно быть прежде всего направлено на реализацию и усиление контрольно-советующих функций аудита. Такое расширение границ аудиторской деятельности может быть достигнуто только в результате перехода от модели подтверждающего к модели системно-ориентированного аудита путем вовлечения в теорию и практику аудита информационных технологий и разработки и постоянного совершенствования аудиторских стандартов в области планирования аудита в условиях компьютерной обработки данных, оценки риска и внутреннего контроля в среде компьютерной и информационных систем аудируемого субъекта, проведения аудита непосредственно информационных систем организации.

Вместе с тем, на сегодняшний день практически отсутствуют работы, обобщающие разработки российских и западных ученых в данной области, российских и международных стандартов в области аудита, информационных технологий, безопасности информационных систем, позволяющие представить аудит информационных систем как самостоятельное научное направление и заложить основы стандартизации и аттестации данного вида деятельности. Данная работа восполняет определенный пробел в теории и практике российского аудита, так как позволяет сформулировать принципы аудита информационных систем и заложить основы для разработки методики оценки рисков и проведения аудита в условиях компьютерной обработки данных, в связи с чем представляет научный и практический интерес.

Сиротенко Э.А., д.э.н., профессор, зам. зав. кафедрой «Экономический анализ и аудит» Финансовой Академии при Правительстве РФ

## 4.5. METHODOLOGICAL APPROACHES TO AUDIT OF INFORMATION SYSTEMS

O.V. Baranova, the Post-graduate Student of Chair «Economic Analysis and Audit» Finance Academy under the Government of the Russian Federation

The article states timely problems of information systems audit in computer aided environment and describes main approaches to information systems audit both as part of internal control system of the company and a separate target for inspection. The article includes useful information about current methods of information systems audit, contains analysis through comparison with CobiT requirements and description of basic rules of such standards as COSO, ITIL, CMMI.

Moreover reader gets familiar with basic elements of auditor's software which is used during the financial statements audit as means of quality increase.

### Literature

1. Automated information technologies in economy [Text] / prof. G.A. Titorenko. – M.: Unity, 2006.
2. Bakanov M.I. Theory of economic analysis [Text] / M.I. Bakanov, M.V. Melnik, A.D. Sheremet. – M.: Finance and statistics, 2006.
3. O.V. Baranova. Information systems audit in computer aided environment [Text] / O.V. Baranova // Economics and quality management: accounting, analysis, methods, models, instruments and audit. : collection of scientific proceedings. – Tambov : TGTU, 2008.
4. O.V. Baranova. Audit information systems [Text] / O.V. Baranova // Financial business. – 2006. – №2. – pages 53-58.
5. O.V. Baranova. Methodology of audit in computer aided environment [Text] / O.V. Baranova. – M.: Company Sputnik+, 2008.
6. Bychkova S.M., Rastamkhanova L.N. Risks in audit [Text] / S.M. Bychkova, L.N. Rastamkhanova – M.: Finance and statistics, 2003.
7. A. Goremykin. Audit automation [Text] / A. Goremykin // Financial newspaper. – 2005. – №7.
8. M. Davletkhanov. Concept of one-time passwords in authentication system [Text] / M. Davletkhanov // BYTE/Russia. – 2006. – №7-8.
9. Eremin L. Information technology [Text] / L. Eremin // financial newspaper. – 2005. – №27.
10. G.N. Isaev. Information systems in economics [Text] / G.N. Isaev. – M.: Omega-L, 2006.
11. S.N. Komendenko. Approaches to forming audit program [Text] / S.N. Komendenko // Auditor. – 2006. – №1.
12. D. Legezo. The third comes. ITIL v.3 [Text] / D. Legezo // Intelligent enterprise. – 2008. – №2.
13. S.M. Patrushina. Information systems in accounting [Text] / S.M. Patrushina. – M.: IKC «MarT», 2003.
14. V.I. Podolskiy. Computer audit [Text] / V.I. Podolskiy, N.S. Sherbakova, V.L. Komissarov. – M.: UNITY – DANA, 2004.
15. E.A. Sirotenko. Information modeling of audit [Text] / E.A. Sirotenko. – M.: Finance Academy under the Government of the Russian Federation, Orgservice-2000, 2004.
16. E.A. Sirotenko. Perspectives of development of audit theory and methodology [Text] / E.A. Sirotenko // Audit vedomosti. – 2006. – №1. – C. 17-24.
17. G.V. Fedorova. Information technologies of accounting, analysis and audit [Text] / G.V. Fedorova. – M.: Omega - L, 2006.
18. V.V. Hanferyan. Audit and consulting Markey in 2007 [Internet resource] / V.V. Hanferyan // Encyclopedia expert RA, 2008.
19. Book on IT Control Objectives for Sarbanes-Oxley. The Role of IT in the design and implementation of internal control over financial reporting, 2<sup>nd</sup> Edition. – USA: IT Governance Institute, 2006.
20. Cobit Mapping: Overview of International IT Guidance, 2<sup>nd</sup> edition. – USA, IT Governance Institute. – 2006.
21. IT Examination Handbook. Audit. – Federal Financial Institutions Examination Council, 2003.
22. Kristine M. Protzman, Vasant Raval. Concept Mapping – A learning tool for information systems audit profession. // Information systems control journal. Vol. 3. 2004

### Keywords

Audit; internal control system; information system; audit risks; computer aided environment; audit methods; CobiT standard; financial statements risks; audit software; risk assessment.