Сметанко А.В.

ОСОБЕННОСТИ ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА В УСЛОВИЯХ ИСПОЛЬЗОВАНИИ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ УЧЕТА И УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

Постановка проблемы.

В условиях глобальной автоматизации бухгалтерского, управленческого и налогового учета на крупных предприятиях с развитой инфраструктурой возникает практическая необходимость в организации службы внутреннего аудита. Основной проблемой внутреннего аудита корпоративных автоматизированных систем учета и управления является их программная и аппаратная часть.

Пристальное внимание к данным частям корпоративных автоматизированных систем обусловлено в необходимости проверки и контроля используемых технологий установленным требованиям с целью прогнозирования и своевременного выявления внутрикорпоративных ошибок, связанных с защитой информационных систем, вводом и обработкой учетной информации и т.д.

Анализ последних достижений и публикаций.

Изучение и анализ научной литературы и публикаций показал, что вопросы связанные с организацией и методикой проведения внутреннего аудита на предприятиях разных форм собственности практически не раскрыт и находится в стадии динамичного развития.

Попытки провести фундаментальный анализ и раскрыть особенности проведения аудиторских проверок в условиях автоматизированных систем учета и управления предприятием предприняты российскими учеными Романовым А.Н., Одинцовым Б.Е.[2].

Рассмотрение публикаций в периодических и научных журналах показал то, что вопросы, связанные с проведением аудита на предприятиях использующих корпоративные и внутрифирменные системы и технологии обработки учетной информации носят фрагментарный характер основанный на международных положениях и стандартах проведения аудита.

Анализ действующих международных положений и стандартов аудита показал, что основные положения данных нормативов носят рекомендательный характер и раскрывают только ключевые моменты, связанные с организацией и методикой проведения аудиторских проверок в условиях использования информационных систем и технологий в учете и управлении организацией [1].

Формулировка целей статьи.

В статье рассматриваются аспекты организации и методики проведения внутреннего аудита информационно-техническими подразделениями и силами внутренних аудиторов (информатизаторами).

Изложение основного материала.

Повсеместное развитие и внедрение информационных систем и технологий в учете и управлении предприятием требует проведение их аудита. При этом аудит должен давать оценку качества организации, методики и управления предприятием при использовании информационных систем, технологий и бухгалтерских программ, как отдельными структурными подразделениями, так и по отдельным службам и исполнителям. Поэтому для эффективной оценки используемых предприятием информационных систем и технологий требуется выделение отдельного направления аудита информационных систем и технологий, требующего подготовленных специалистов владеющими методами, приемами, инструментариями работы в информационных сетях и специализированных управленческих, бухгалтерских компьютерных программах.

Развитая корпоративная информационная система учета, обработки, анализа и хранения информации требует от руководителей крупных предприятий создания службы внутреннего аудита. Данная служба должна осуществлять проверку и оценку разных сторон деятельности информационных подразделений собственными силами. Создание данной службы направлено на устранение недостатков связанных с проверками официальных аудиторов или контролирующих органов, а также необходимостью прогнозирования и своевременного выявления ошибок, возникающих как при вводе, обработке информации, так и на стадиях разработки и внедрения программных продуктов в управлении предприятием, которые в последствии окажут непосредственное влияние на принятие управленческих решений.

Осуществление проверки операционной деятельности любого крупного предприятия независимо от форм собственности необходимо для получения полной и объективной картины подверженности данной организации определенным рискам, связанным с использованием внутрикорпоративных компьютерных систем и специализированных компьютерных программ обработки учетной информации.

Для выявления недостатков связанных с технологией обработки, анализа и хранения информации по средствам управления информационных систем требует от внутренних аудиторов проверки следующих составных корпоративной информационной системы:

алгоритма ее работы;

архитектуры корпоративной информационной системы;

схемы построения локальной и внутрикорпоративной сети;

организации и методики выгрузки-загрузки учетной информации по средствам распределенной обработки данных;

прав и обязанностей пользователей, выполняющих ввод, обработку, анализ и архивирование учетной и управленческой информации;

программного обеспечения, отвечающего за защиту от проникновения в корпоративную базу данных;

организацию, разработку и сопровождение программного обеспечения и баз данных;

надежность программного обеспечения сторонних разработчиков;

готовности к нестандартным и внештатным ситуациям, связанным с выходом из строя сервера или АРМ;

договора с контрагентами по вопросам обслуживания вычислительных сетей, техники и т.д.

На стадии организации внутреннего аудита особое требование должно предъявляться проверяющим в части квалифицированности, независимости аудиторов от других структурных подразделений, качества подготовки рабочей документации к проверке, контроля исполнения аудиторских решений и т.д.

Основной составляющей организации внутреннего аудита является составление плана и детализированного перечня направлений проверки, который требует профессиональных знаний, навыков и опыта работы внутренних аудиторов. В том случае если во внутренней службе аудита недостаточно или вообще отсутствуют специалисты по определенному направлению проверки, то возникает объективная необходимость в привлечении специалистов со стороны. При таком подходе ключевыми становятся вопросы правильной организации проверок, которые должны выполняться проверяемыми специалистами под методологическим руководством специалистов внутренней службы аудита.

При проведении внутреннего аудита, проверки не должны мешать текущей работе предприятия, т.е. не должно быть несогласованных остановок работы пользователей, блокировок, отсутствия доступа к информации, изменения и нарушения целостности базы данных и т.д. Следует отметить, что согласованных прерываний работы должно быть минимальное количество. При этом для работников отдельных проверяемых служб и подразделений не должны создаваться дополнительные нагрузки и обязанности.

Особое внимание аудиторов при проведении проверок на предприятиях использующих корпоративную систему обработки информации должно быть направленно на сохранение коммерческой тайны и корпоративной информации. Разветвленные компьютерные сети, имеющие определенную цифровую защиту и шифрование, требуют от аудиторов запрета на открытие доступа к учетной информации, получения кодов и электронных цифровых подписей к закрытой информации. Данное сохранение достигается путем разграничения прав доступа аудиторов и специалистов к определенному массиву информации или корпоративной базы данных. Поэтому механизмы парольной защиты, санкционирования доступа и разграничения прав при проведении внутреннего аудита не должны выключаться.

При проверке правильности конструктивного или технологического решения аудиторам достаточно провести выборочные проверки на типовых задачах или АРМ специалистов, бухгалтеров, руководителей.

При анализе отсутствия недоработок и некорректной реализации проверки должны быть сплошными. В этом случае у проверяющих возникает большой объём работы, справиться с которым возможно посредством выделения этапов и создания согласованного поэтапного графика работ.

Следует отметить, что аудит соответствия должен базироваться на документарных проверках и аналитической работе основанной на обязательной проверке средств и технологий контроля информационных систем и технологий. При этом глубина всех аудиторских проверок должна быть максимальной.

После анализа организационных мероприятий, документации и электронных служебных файлов, аудит информационных технологий должен быть переведён в тестовый режим их проверки. При проведении тестирования и технических проверок, аудиторам необходимо иметь в виду наличие человеческого фактора. В качестве тестирования аудиторы могут смоделировать ситуации когда человек на своем экране может видеть проникновение в компьютер или необычно сетевую активность пользователей, изменение интерфейсного окна пользователя и т.д. Данные попытки тестирования направлены на определение реакции конкретного человека на внештатную работу. Проверки фактического состояния информационных технологий могут состоять из выполнения заранее согласованных тестовых примеров, администраторских команд, а также из несанкционированных вмешательств в работу информационной системы. Данные задания, тесты и внештатные ситуации должны быть согласованы на организационно-подготовительной стадии аудиторской проверки. На данной стадии определяются вопросы, которые аудиторы намерены выяснить, а также что именно должно быть проверено, в каком объёме и в какие сроки.

Подготовительная стадия аудита определяет состав конкретных тестовых примеров, перечень конкретных вмешательств в работу информационной системы, а также устанавливается минимальный круг должностных лиц, кто должен знать о тест-проверках.

При проведении тест-проверок на доступ к критическим разделам информации аудиторы и ответственные должностные лица должны предусмотреть варианты восстановления информации в случае ее нарушения, а также осуществить контроль за работниками служб отвечающими за ее сохранность.

На организационно-подготовительной стадии аудита следует провести разграничение прав и обязанностей между проверяющими и проверяемыми. При данном разграничении, аудитор согласовывает с руководителем или начальником отдела в каком виде будет предоставлена информация, связанная с проведением проверки, а также в каком виде и к какой информации будет предоставлен доступ аудитору.

Следует отметить, что при разработке и внедрении корпоративных систем и технологий обработки учетной информации и управлением предприятием программистам и другим ответственным лицам следует создавать благоприятные условия необходимые для успешного проведения внутреннего аудита. Для этого необходимо создавать такую форму ввода и обработки информации которая бы позволяла осуществлять контроль и давала бы пользователям возможность смотреть на совершаемые процессы с точки зрения аудиторов. Данная форма контроля в дальнейшем позволит сократить и минимизировать трудозатраты аудитора, а также снизить уровень аудиторского риска.

Объёмы и последовательность проверок в каждом конкретном случае определяются в зависимости от заданной темы. Общим процессом для всех случаев проведения аудита является оформление его результатов. Прежде всего, ход работ, их промежуточные результаты, оценку и описание фактов и явлений следует отражать в рабочих документах аудитора, данные из которых по окончанию проверки обобщаются и выносятся в аудиторское заключение.

Следует отметить, что окончательные оценки по результатам аудита могут быть представлены в нескольких видах: самое общее текстовое заключение, табличные оценки на основе промежуточных оценок, оценки в виде рейтингов и т.д. При подведении итогов следует предусматривать анализ материалов предыдущих проверок с целью выяснения, не возникают ли повторяющиеся проблемы.

По отношению к окончательным результатам проверяющие должны выполнять требование соблюдения конфиденциальности и недопустимости разглашения общих результатов и того рабочего состояния, которое они установили. Поэтому должны быть проработаны корпоративные требования к формам и объёмам высказывания проверяющими собственного мнения о проверках, общих оценках и о качестве работы проверяемых.

Заключительным этапом внутреннего аудита корпоративных информационных систем и технологий является разработка согласованного плана мероприятий по устранению недостатков, замечаний, реализации рекомендаций и т.д. Основное требование к этому этапу работ – конкретизация действий, сроков и ответственных исполнителей, а также обязательность отчёта ответственных исполнителей о выполнении мероприятий, являющихся безусловно необходимыми и выработанными ценой общих усилий проверяющих и проверяемых.

Вывод.

Исследование автором особенностей проведения внутреннего аудита при использовании корпоративных автоматизированных систем учета и управления предприятием позволяют сделать следующие выводы:

- анализ международных стандартов аудита свидетельствует, о поверхностном определении основных стадий и этапов проведения аудита в условиях автоматизированных систем и технологий обработки учетной информации и управлением предприятием;
- при высокой степени отлаженности процессов подготовки и проведения проверок, а также подведения их результатов внутренний аудит в рамках корпоративных информационных систем и технологий следует организовывать по каждому факту или этапу работ;
- разработка и внедрение корпоративных информационных систем и технологий должна осуществляться с таким расчетом, что при вводе, обработке и анализе информация должна проходить определенную стадию контроля тем самым создавая благоприятные предпосылки к снижению человеческого фактора допущения ошибок и повышения эффективности проведения аудита;
- для успешного проведения внутреннего аудита отделом информационного обеспечения предприятия следует создать примерный перечень направлений проведения проверки:

Ø наличие должностных инструкций, определяющих обязанности сотрудников;

Ø наличие утверждённых планов работ;

Ø требования предъявляемые к АРМ и сотрудникам осуществляющих за ними работу;

Ø список почтовых и сетевых адресов АРМ корпоративной информационной системы;

Ø учет трафика передачи данных по локальной и внешней сети;

Ø перечень программного обеспечения, которое может быть установлено на сервер и АРМ;

Ø наличие утверждённой документации на программное обеспечение к информационной системе учета и управления;

Ø структура и схема передачи и обработки данных по вычислительным сетям корпоративной информационной системы;

Ø оформление, учёт и исполнение заявок на создание АРМ, установку программного обеспечения и информационных ресурсов;

Ø наличие и правильность ведения паспортов на АРМ

Ø наличие на АРМ, обрабатывающих информацию “корпоративная или коммерческая тайна”, технических средств защиты информации, организация администрирования средств защиты информации;

Ø наличие и правильность ведения учёта и архивов программ самостоятельной разработки;

Ø хранение эталонного программного обеспечения;

Ø наличие программных средств, технологий и инструкций связанных с восстановлением информации и работоспособности системы при возникновении внештатных ситуаций;

Ø организация антивирусной защиты и парольной защиты корпоративной информации.

Источники и литература

1. Романов А.Н., Одинцов Б.Е. Автоматизация аудита. М.: Аудит, ЮНИТИ, 1999г.
2. Международные стандарты аудита и Кодекс этики профессиональных бухгалтеров (1999). – М.:[издательство], 2000. – 699 с.