УДК 657.6

Л.А.СЕРОБАБА
Харьковская национальная академия городского хозяйства

УПРАВЛЕНИЕ РИСКАМИ В ПРОЦЕССЕ АУДИТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Подчеркивается важность минимизирования негативного влияния рисков на достижение целей организации. Рассмотрены риски применительно к аудиту информационных технологий, их специфика и методы управления ими.

Среди специалистов в области информационной безопасности, обеспечения непрерывности бизнеса и управления качеством сравнительно недавно появились, но уже прочно укоренились понятия «оценка рисков информационной безопасности» и «управление информационными рисками». В мировой практике такая оценка применяется для снижения рисков управления, а точнее сказать, ответственности персонала за внезапно возникшие проблемы [4]. Угрозы безопасности носят вероятностный характер и изменяются в процессе жизнедеятельности компании. Идентифицируя соответствующие угрозы, анализируя сопутствующие риски и принимая затем эффективные контрмеры, удается избежать риска, смягчить его, передать риск третьему лицу в виде эффективной программы страхования. Лица, заинтересованные в успешном функционировании организации (включая инвесторов), все больше обращают внимание на минимизацию негативного влияния рисков на достижение целей организации, и, следовательно, на подтверждение исполнительным руководством наличия и эффективного функционирования системы управления рисками.

Одним из общепринятых в современной деловой практике способов подтверждения существования и успешного функционирования системы управления рисками является аудит, в частности аудит корпоративных информационных систем.

Главное предназначение любого аудита, прежде всего, в предоставлении руководству организации объективной информации о текущем состоянии основных ресурсов (активов) и степени адекватности процедур и средств контроля целям, задачам и требованиям основной деятельности организации. Аудит информационных технологий (аудит ИТ) решает аналогичные задачи в отношении информационных, программных и технических компьютерных ресурсов организации с учетом их специфических особенностей.

Развитие информационных технологий и их проникновение в деятельность организаций привели к тому, что эффективность управления предприятием в значительной степени зависит от характеристи-

ки информации, используемой для принятия решений. Аудит ИТ является одним из способов получения такой информации. Предоставляемая в результате аудита информация позволяет оценить эффективность и качество использования ресурсов организации. Необходимо осознавать, что регулярный аудит является неотъемлемой частью эффективного управленческого процесса. Для принятия адекватных управленческих решений исходная информация, кроме объективности, должна соответствовать требованиям достоверности и качества. Указанные требования могут быть выполнены только при условии достижения приемлемого уровня воздействия негативных факторов (угроз), влияющих на характеристики информации.

В традиционной практике управленческой деятельности угрозы часто рассматриваются, в первую очередь, применительно к основным производственным процессам (бизнес-процессам). Но при этом из поля зрения нередко выпадает то важное обстоятельство, что и сам процесс управления в целом (как и его составные части) в большой степени подвержен влиянию различных угроз, поскольку он в недостаточной степени формализуется и сильно зависит от проявлений «человеческого фактора». Это означает, что возможность наступления случаев реализации таких угроз обычно оценивается через вероятностные, а не абсолютные показатели реализации рисков. По определению Международной Ассоциации аудита и контроля информационных систем (ISACA) [2], «риск – это вероятность совершения действия или наступления события, проявляющего негативный эффект в отношении организации (предприятия) и его информационных систем».

Как составная часть процесса управления предприятием, аудит ИТ, в свою очередь, также подвержен влиянию рисков. Для снижения рисков применяются различные методики управления ими.

Риски, связанные с проведением аудита ИТ, условно разделяют на:

- проектные риски;
- риски предметной области, или ИТ-риски;
- процессные риски (риски аудита), т.е. риски, отражающие специфику процессов аудита ИТ [3].

Следует заметить, что по способу организации работ аудит ИТ относится к проектной деятельности, поскольку каждый аудит:

- инициируется и санкционируется руководством предприятия;
- характеризуется четко определенными временными рамками и конкретными задачами;
- требует выделения ресурса, в зависимости от сложности и объема задач, для достижения поставленных целей.

Все указанные выше моменты относятся именно к проектной, а не операционной деятельности, поскольку «проект – это комплексное, неповторяющееся, одномоментное мероприятие, ограниченное по времени, бюджету, ресурсам, а также четкими указаниями по выполнению, разработанными под потребности заказчика» [3].

По мнению специалистов в области управления рисками [4], наиболее характерными для проекта аудита ИТ являются:

- Риск неправильного планирования проекта, в том числе неправильное планирование ресурсов, продолжительности и этапов проекта в условиях диктата заказчика и руководства исполнителя, ориентировки на конкретных экспертов, в то время как они недоступны, и т.д.
- Организационно-управленческий риск. Например: недостаточная поддержка проекта руководством заказчика и/или исполнителя, неэффективная структура проектной команды и т.п.
- Риск изменения границ проекта. Например: недостаточно четкое определение требований в начале проекта, изменение требований в ходе проекта и т.п.
- Риск персонала. Например: более долгое, чем планировалось, формирование проектной команды, низкая производительность и мотивация персонала проектной группы, сопротивление персонала заказчика своевременной передаче достоверной информации и т.п.
- Процессный риск. Например, избыточный объем канцелярской переписки, избыточная или, наоборот, недостаточная формальность проектных процедур и т.д.
- Общий риск провала проекта. Например, при смене руководства заказчика в ходе осуществления проекта и т.п.

Традиционно аудит информационных технологий и систем в существенной мере ограничивается рассмотрением вопросов информационной безопасности и контроля, включая:

- системы физического и логического контроля доступа к ИТ-оборудованию;
- системы сетевой безопасности;
- системы контроля прикладных программ;
- системы планирования непрерывности деятельности и т.п.

В стандартной практике, при аудите ИТ риски анализируются с точки зрения решения общей задачи обеспечения безопасности, включая задачи обеспечения конфиденциальности, целостности и доступности информационных систем (программно-технических комплексов, сетей передачи данных и т.д.) и собственно информации, которую они хранят, передают и обрабатывают. Для качественного выполнения

этих задач аудитор, проводящий оценку рисков, должен обладать глубоким пониманием специфики систем обработки информации и особенностей технологий их реализации.

Отсюда следует, что при оценке ИТ-рисков, в первую очередь собирается информация, собственно относящаяся к системам обработки информации, которая классифицируется следующим образом:

- технические средства;
- программное обеспечение;
- системные интерфейсы (внешние и внутренние связи);
- данные и информация;
- персонал поддержки и эксплуатации;
- критичность систем и данных (например, важность систем для организации);
- чувствительность систем и данных (классификация соответствует [5]).

Однако если рассматривать риски ИТ только в рамках технологий и информационной безопасности, это не позволит ИТ-аудитору оценить бизнес-риски, связанные с применением информационных ресурсов, и их влияние на достижение целей организации. Существующие тенденции таковы, что с течением времени ИТ во все большей степени проникает в различные аспекты деятельности организации, приобретая стратегическое значение. При этом текущее состояние ИТ-ресурсов, а также степень их использования в основной деятельности организации, часто оказывают непосредственное влияние на финансовые результаты компаний и их позицию на рынке. Поэтому аудитору необходимо понимать, что риски, связанные с ИТ, не ограничены критериями информационной безопасности, целостности и достоверности данных аудита. Последнее утверждение верно, только если условия контракта на проведение аудита ИТ в явном виде не ограничивают круг вопросов такой тематикой.

Таким образом, следуя текущим реалиям, надо обращать внимание на необходимость оценки существенного риска – риска неэффективности самих ИТ-систем. Задача измеримости выгод от применения ИТ не всегда может быть решена непосредственно в количественных показателях, так как это понятие измеряется не только в значениях возврата инвестиций и окупаемости затрат. При проверке реализации преимуществ ИТ аудитору рекомендуется получить ответ на следующие вопросы:

- Насколько хорошо ИТ обслуживает основную деятельность предприятия?

- Каков показатель эффективности ИТ для основной деятельности на определенную дату?

Оценка риска самого процесса аудита и его результатов в настоящее время приобретает все большее значение для специалистов по управлению рисками. Понятие риска играет сегодня ключевую роль в мире аудита. Вся аудиторская деятельность заключает в себе определенный уровень риска, поскольку активы компании могут быть неправильно оценены, или аудитор не сможет обнаружить ошибки или мошеннические действия. Кроме того, эти проблемы могут возникнуть из-за неадекватных выборок аудитором тестовых данных во время определения уровней рисков или ошибок. Об актуальности оценки аудиторского риска свидетельствует тот факт, что данному вопросу уделяется внимание, по меньшей мере, в шести из действующих на сегодня международных нормативов аудита [1].

В «Методических рекомендациях Международной ассоциации аудита и контроля информационных систем (ISACA) по оценке риска при планировании аудита ИТ» [2] для аудита ИТ рекомендуется применять те же базовые методы, что и для аудита финансовых систем. Там же указывается, что для оценки общего риска необходимо производить оценку по типам риска: внутренний риск, риск средств контроля, риск необнаружения. Все эти компоненты входят в универсальную модель риска аудита, учрежденную под эгидой «Общепринятых стандартов аудита» (GAAS – Generally Accepted Auditing Standards). Эта модель позволяет аудиторам учитывать различные обстоятельства при выборе собственного подхода к аудиту. Так, согласно этой модели, аудитору необходимо понимать специфику:

- основной деятельности организации-заказчика и отрасли, к которой она относится;
- систем обработки информации;
- квалификации персонала;
- политики и процедур предприятия.

Кроме этого, аудитору следует обращать внимание на внутренние процедуры контроля, проверять эффективность этих средств контроля, применяя, при необходимости, доказательное тестирование, а также оценивать риски мошенничества.

На основе оценки различных рисков и тестирования средств контроля аудитор выносит официальное заключение о группе фактов, необходимых для достижения «разумной гарантии» достаточности средств контроля, обеспечивающей приемлемый уровень рисков.

Математически модель (методика расчета) риска аудита представляется зарубежными экономистами [6, 7] следующим образом:

$$AR = IR \times CR \times DR,$$

где *AR* (Audit Risk) – общий риск аудита. Риск того, что аудитор вынесет неправильное аудиторское заключение (суммарный или итоговый риск); *IR* (Inherent Risk) – внутренний (присущий) риск. Риск появления существенной ошибки при проведении аудита (отдельной или в комбинации с другими ошибками), при условии, что соответствующие процедуры внутреннего контроля отсутствуют. Например, внутренний риск, связанный с безопасностью операционной системы (ОС) на сервере, обычно высокий, поскольку несанкционированное изменение общих данных или даже просто получение к ним доступа через уязвимости ОС могут привести к искажению управленческой информации и снижению конкурентоспособности компании. В противоположность ему, внутренний риск, связанный с безопасностью отдельной рабочей станции (естественно, когда доказано, что она не применяется в критически важных процессах), обычно низкий.

Внутренний риск для большинства информационных систем обычно оценивается как высокий, поскольку потенциальный эффект ошибок распространяется параллельно на несколько систем и затрагивает много пользователей – из-за того, что большинство применяемых систем относятся к категории систем совместного пользования.

CR (Control Risk) – риск средств контроля. Риск того, что одиночная или комбинированная ошибка аудитора не будет своевременно предотвращена, обнаружена или исправлена системой внутреннего контроля.

Например, риск средств контроля, ассоциированный с просмотром электронного журнала операций «вручную», будет выше, чем с применением автоматизированных средств, из-за вероятности пропуска нужной информации, если объем этой информации достаточно большой.

Аудитору рекомендуется оценивать риск средств контроля как высокий, в случае если внутренние процедуры контроля:

- не идентифицированы;
- не оценены как эффективные;
- не протестированы или тесты не доказали их адекватность и правильное функционирование.

DR (Detection Risk) – риск необнаружения. Риск того, что процедуры доказательного тестирования (выборочной проверки), осуществляемые аудитором, не обнаружат существенных ошибок (как отдельных, так и комбинированных). Например, риск необнаружения, ассоциированный с идентификацией нарушений системы безопасности прикладной программы, обычно оценивается как высокий, если элек-

тронный журнал был недоступен в течение всего периода аудита. Риск необнаружения, связанный с планом восстановления деятельности после нештатных ситуаций, обычно оценивается как низкий, так как его наличие или отсутствие легко устанавливается.

Чем выше оцениваются внутренний риск и риск систем контроля, тем больше свидетельств аудитор ИТ должен получить в результате доказательных процедур аудита. При анализе рисков следует обратить внимание на то, что внутренний (присущий) риск и риск систем контроля относятся к рискам, контролируемым клиентом (организацией, где проводится аудит), а риск необнаружения относится к рискам, контролируемым аудитором.

Несмотря на использование строгого математического выражения при указании зависимостей между различными видами рисков, в реальности заключение аудитора преимущественно носит характер экспертной оценки. Основная задача управления рисками в процессе проведении аудита ИТ сводится к необходимости достижения минимального значения суммарного риска. При этом условии будет достигнута разумная гарантия того, что аудиторское заключение свободно от существенных ошибок.

В заключение следует отметить, что в отсутствие методологии управления рисками оценка рисков аудита будет восприниматься субъективно и основываться на предположениях. По сути, такая оценка в довольно большой степени будет зависеть от видения, подхода, образованности и опыта отдельного эксперта (или группы экспертов), проводящего оценку рисков.

1.Аудит: Практическое пособие / Под ред. А.Кузьминского. – К.: Учетинформ, 1996. – 283 с.

2.ISACA «IS Auditing Guideline, Use of Risk Assessment In Audit Planning», Document G13; 2000.

3.Грей Клиффорд, Ларсон Эрик. Управление проектами: Пер. с англ. – М.: Дело и сервис, 2003.

4.Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность. – М.: ДМК Пресс, 2005. – 384 с.

5.Risk management Guide for Information Technology System, NIST, 2002.

6.Рой Додж. Краткое руководство по стандартам и нормам аудита. – М.: Финансы и статистика, 1992. – 240 с.

7.Робертсон Дж. Аудит. – М.: Контакт,1993. – 496 с.

Получено 28.05.2007