Станислав Митрович
доктор экономических наук, Университет в г. Нови-Сад
(Республика Сербия)
(e-mail: Mitrovic.Stanislav@hotmail.com)

ОБ ОЦЕНКЕ РИСКОВ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ В ЭКОНОМИЧЕСКОМ АНАЛИЗЕ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИЙ

В статье излагается метод самооценки информационных систем как действующий инструмент внутреннего контроля в системе управления бизнес-процессами организаций. Основные результаты исследования автора подтверждают гипотезу о том, что применение методики самооценки систем информационных технологий организаций для обеспечения финансовой и операционной отчетности хозяйственной деятельности находится в прямой корреляции с ростом эффективности экономического анализа и обеспечения достоверности его результатов и выводов.

Ключевые слова: современные информационные технологии, информационные системы, экономический анализ, оценка рисков, самооценка.

DOI: 10.31857/S020736760000814-4

Успешное развитие компании в современных экономических условиях возможно только тогда, когда каждый ее сотрудник в дополнение к основной деятельности постоянно совершенствует существующие процессы. Именно эта задача, по мнению руководителей многих организаций, позволяет оптимизировать деятельность как отдельных работников, так и компании в целом, способствуя выявлению «проблемных» процессов или процессов, «отживших свой век», и представляет собой источник развития бизнеса [7].

Управление бизнес-процессами в текущих условиях требует от собственника компании широкого применения различных методов анализа экономической информации, в том числе для оценки и минимизации рисков, как в специфических сегментах, так и в общей системе корпоративного управления. Современные информационные технологии (ИТ) кардинально изменили возможности для совершенствования экономического анализа, сокращения времени принятия решений, гармонично дополнив новыми возможностями методологию стратегического и оперативного менеджмента. Развитие информационных технологий дало возможность бизнесу разрабатывать эффективные системы экономического анализа. Однако, несмотря на свойства оперативности и предоставляемые ими возможности обработки большого количества информации и моделирования стратегических решений, большинство из информационных систем имеет такие недостатки как отсутствие прозрачности, высокая уязвимость и подверженность риску на разных стадиях

внедрения и эксплуатации. Таким образом, создается ситуация, в которой современные информационные системы, с одной стороны, являются двигателем прогресса в области экономического анализа хозяйственной деятельности организаций, а с другой стороны – источником риска в экономической области.

В этой связи особенно актуальным становится вопрос оценки, управления и минимизации рисков в информационной области. Информационные системы, функционирующие в сфере экономического анализа, где речь идет о системе информационных и экономических данных как основе деятельности компании и ее конкурентном преимуществе, должны быть обеспечены специализированной подсистемой безопасности с конкретными свойствами. Однако в российских условиях анализ рисков в данной сфере если и осуществляется, то, как правило, выполняется пока еще формально, с применением произвольных методик, в отличие от практики зарубежных стран. Вопросам анализа рисков в информационной области в зарубежной методике и практике уделяется значительное внимание, и уже десятилетиями собирается статистика для анализа проблем и рисков, совершенствуются и развиваются методические инструменты. Но глобальная проблема оценки рисков в информационной сфере остается актуальной для компаний во всем мире – темпы технологического прогресса в области ИТ таковы, что для новейших технологий оценочных инструментов, в полной мере позволяющих оценить риски в исследуемой области или, как минимум, позволяющих адаптировать оценочные инструменты к темпам развития технологий, по оценкам исследователей, пока не существует [6. С. 315].

В последние годы ситуация начинает меняться в сфере внедрения информационных систем в экономическую деятельность организаций и в России. Среди российских специалистов зреет понимание необходимости подобной деятельности на регулярной основе – то есть речь идет не о выявлении рисков перед началом того или иного проекта, что, безусловно, является важным и неотъемлемым этапом, а о регулярной оценке, мониторинге и управлении рисками на протяжении внедрения информационного решения и его тестирования, а также дальнейшего функционирования в системе экономического анализа организации. Наибольшую активность в данной области проявляют банковские, страховые и крупные коммерческие структуры, которые серьезно заботятся о безопасности своих информационных и финансовых ресурсов и имеют для этого необходимые резервы.

Целью анализа рисков, связанных с эксплуатацией информационных систем, функционирующих в сфере экономического анализа организации, является «оценка угроз (т. е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также определение комплекса контрмер, обеспечивающего достаточный уровень защищенности системы» [1].

В условиях прогрессирующего развития методического обеспечения теории рисков и повышения в данном контексте требований к определению рисков в современной науке и практике в сегодняшних условиях все более остро встает вопрос об осуществлении процедуры самооценки (Control Self-Assessment – CSA), как одного из возможных практических методов с большим потенциалом для выявления рисков, связанных с применением информационных технологий в экономическом анализе хозяйственной деятельности организаций.

В связи с этим становится очевидным, что формирование и развитие методики самооценки информационных технологий на научной основе, применяющейся для целей экономического анализа хозяйственной деятельности организаций и повышения эффективности внутреннего контроля, теоретические основы которых на данном этапе находятся на ранних стадиях формирования, дают возможность не только снизить корпоративные риски, но и повысить инвестиционную привлекательность компании, что является конкурентным преимуществом организаций во всех сферах бизнеса [8].

Исходя из этого основная гипотеза нашего исследования была сформулирована следующим образом: применение методики самооценки систем информационных технологий организаций, которые используются хозяйственными организациями для обеспечения бухгалтерского и статистического учетов, финансовой и операционной отчётности находится в прямой корреляции с ростом эффективности экономического анализа и обеспечения достоверности его результатов и выводов, при условии, что методический инструментарий самооценки а) основан на учете основных положений теории риска и самооценки, б) базируется на анализе позитивного опыта методических разработок в области проведения процедур самооценки в организации, в) сопровожден релевантным алгоритмом имплементации.

Процедура самооценки (Control Self-Assestment – CSA) в области применения ИТ-систем в экономическом анализе в нашем исследовании рассматривается как всесторонний и системный анализ деятельности и результатов работы ИТ-систем по выбранным критериям. В данном контексте метод самооценки трактуется как часть системы внутреннего контроля, направленной на совершенствование деятельности организации и, в частности, на выявление и оценку рисков, слабых сторон в работе организации и формулировку рекомендаций для улучшения и повышение эффективности систем и процессов.

В данном контексте в качестве основополагающих положений, свидетельствующих о научной разработанности изучаемой проблемы в современной науке и выступающих теоретической и методологической базой исследования, нами выделяются:

1) теория риска, основные составляющие которой, зародившись еще в 20-х гг. XX в., получили научную разработку на Западе в 1980-е – начале 1990-х гг., и которая, по мнению исследователей [2], остается на сегодняшний день одной из самых проблемных областей во внутреннем контроле;

2) типовые положения и стандарты, регулирующие вопросы внутреннего аудита, внутреннего контроля и самооценки организации и определяю-

щие ее как важнейший инструмент непрерывного улучшения деятельности организации и предупреждения рисков (ISA (в особ., ISAs 200, 220, 315, 320, 330, 300, etc.), ICA (в особ., 2100, 2120) [9, 10], модели (COSO [5], Deming 1951 [4], Conti 2000 [3], и т.п.).

Как показывают результаты нашего исследования, введение самооценки в информационную сферу является одним из основных инструментов для определения ключевых факторов рисков, относительно применения современных информационных технологий для целей ведения бухгалтерского и статистического учетов и составления финансовой отчетности, что особенно важно с точки зрения обеспечения эффективности экономического анализа деятельности организации. Помимо этого, важным направлением в процессе применения самооценки является и направленность на предоставление объективных гарантий в отношении системы управления рисками в информационной сфере, которая также является ключевым и необходимым (обязательным) условием для дальнейшего применения данной процедуры в качестве инструмента управления эффективностью хозяйственной деятельности организацией.

Предложенная методика применения процедуры самооценки информационной системы организации, которую мы рассматриваем в данной статье, предполагает использование алгоритма из четырех шагов:

1. Подготовка процедуры самооценки, которая включает в себя определение ключевых элементов информационной системы, для которых необходимо провести самооценку, отбор вопросов для каждого элемента риска, разработку инструкции по заполнению анкеты и определение круга сотрудников компании, которые будут участвовать в анкетировании.

2. Сбор и предварительная обработка данных. В качестве основного метода сбора информации в процессе самооценки информационной системы обычно используется вопросник (анкета) и интервью. Этот этап включает в себя также предварительную обработку данных и подготовку «диагностической» таблицы результатов самооценки.

3. Проверка правильности и определение коэффициента достоверности полученных результатов в ходе проведения процедуры самооценки. Ключевая часть алгоритма по применению процедуры самооценки информационной системы, обладающая большим потенциалом **с** точки зрения повышения объективности в измерении риска и подтверждения роли процедуры самооценки в отношении предоставления гарантий касается дополнительного тестирования результатов самооценки. В результате дополнительного тестирования выборки возможно введение специальных коэффициентов достоверности (надежности) полученных ответов для всей популяции, что нами рассматривается как один из способов преодоления проблемы ошибочных (ложных) утверждений, которые могут дать ложное представление о ситуации в области, являющейся предметом самооценки.

4. Итоговый анализ результатов самооценки и составление отчета. На этом этапе оформляется отчет, содержащий анализ текущего состояния информационной системы и предложения по переходу на более высокий уровень эффективности и защищенности от рисков. На основании выяв-

ленных проблем определяются сроки и методы (план действий) по совершенствованию ключевых областей информационной системы, которые были определены как проблематичные.

В основе процедуры самооценки информационной системы лежит постулат о необходимости создания устойчивой системы управления рисками, которая основана на нескольких взаимосвязанных компонентах, среди которых выделяем: определение и классификация ключевых направлений бизнеса; управление рисками; инструменты и подходы (методы) оценки рисков; управленческая информация; навыки, ресурсы, обучение; непрерывное совершенствование, пользователи ИТ-систем и требования к аналитическому сопровождению хозяйственной деятельности организаций. В процессе разработки методики применения процедуры самооценки в рамках нашего исследования был добавлен дополнительный компонент, относящийся к оценке результатов самооценки – коэффициент достоверности полученных результатов.

Как показала практика, отсутствие именно этого компонента влечет за собой потенциальные проблемы, которые могут значительно снизить эффект от проведения процедуры самооценки, в частности, снизить уровень надежности и объективности результатов самооценки, эффективность управления рисками, привести к неправильной оценке уровня управления ИТ-системой и уменьшить потенциал совершенствования в целом информационной сферы организации. По этой причине проверка правильности и определение коэффициента достоверности полученных в результате проведения процедуры самооценки ответов рассматривается как ключевая часть алгоритма с точки зрения повышения эффективности и надежности, относительно возможностей информационных систем в сфере бухгалтерского и статистического учета, отчетности и экономического анализа деятельности организации.

Обобщая все вышеперечисленные аспекты, можно сделать вывод, что процедура самооценки систем информационных технологий организаций в контексте нашего исследования рассматривается с точки зрения двух ее важнейших функций:

1) в качестве процедуры, призванной обеспечить объективность в оценке системы управления рисками информационных технологий;

2) как эффективный инструмент управления и повышения эффективности результатов организацией, включая и аспект улучшения экономического анализа деятельности.

Таким образом, мы можем подтвердить основную гипотезу данного исследования: применение методики самооценки систем информационных технологий организаций, которые используются для обеспечения бухгалтерского и статистического учетов, финансовой и операционной отчётности хозяйственной деятельности организаций находится в прямой корреляции с ростом эффективности экономического анализа и обеспечения достоверности его результатов и выводов.

Приоритетным направлением дальнейших исследований в области применения процедуры самооценки ИТ-систем организаций мы считаем со-

вершенствование специализированного инструментария для количественного измерения рисков. Практика показывает, что самооценка может приносить существенные результаты в самом начале процесса создания полноценной системы управления рисками с точки зрения формирования базового представления о рисковом профиле, степень адекватности которого зависит от качества информации и степени детализации. Тем не менее, для создания полноценной системы управления рисками ИТ-систем нецелесообразно ограничиваться использованием только данного инструмента, принимая во внимание тот факт, что ни один из методов, используемых на практике, не является единственно возможным. Процессу применения всегда должен предшествовать предварительный анализ, ясное определение целей, сбалансированное и объективное рассмотрение собственных возможностей и планируемых расходов, расчет стоимости ресурсов и реальная оценка необходимого времени. Вследствие зависимости между точностью качественной оценки рисков ИТ-систем, с одной стороны, и квалификации и опыта экспертов, с другой, необходимо также осуществлять логический переход к более точным (по сравнению с преобладающими на данный момент в практике методами) количественным методам измерения рисков в области применения ИТ-систем в компаниях, построению унифицированных экономико-математических моделей, дающих возможность прогнозирования и получения результатов, которые больше основаны на эмпирических данных, нежели на оценках экспертов. Данные аспекты определяют дальнейшие направления исследования проблемы в перспективе и требуют междисциплинарной интеграции научного потенциала для их решения.

Литература

1. *Симонов С.* Современные технологии анализа рисков в информационных системах [Электронный источник] // PCWeek.Ru. URL: https://www.itweek.ru/infrastructure/article/detail.php?ID=59394 (дата обращения: 14.03.2018)
2. *Aldersley S.J.* Discussion on achieved audit risk and the outcome space // Auditing: A Journal of Practice and Theory: Supplement. 1989. Pp. 85-97.
3. *Conti T.* Organizational Self-Assessment // Roma: Pelita press. 2000.
4. *Deming E.* Brought the Quality Revolution to America // L.: Penguin, 1951.
5. Enterprise Risk Management Integrated Framework, COSO [Электронный источник] // The Committee of Sponsoring Organizations of the Treadway Commission. 2004. URL: http://erm.coso.org/ (дата обращения: 20.03.2018).
6. *Jakob H.I., Lars M., Peter A. N.* Managing risk in BA process improvement // N.Y.: MIS. 2017.
7. *Mescon M., Albert M., Khedouri F.* Management: Individual and Organizational Effectiveness // N.Y. Harpercollins College Div. 1985.
8. *McNamee D.* Business Risk Assessment // Altamonte Springs. Florida: Institute of Internal Auditors. 2006.
9. ISAs: List of Standards. [Электронный источник]// The International Federation of Accountants. URL: http://www.ifac.org (дата обращения: 15.03.2018).
10. ICA Standards. [Электронный источник] // The International Compliance Association. URL: http://www.int-comp.org (дата обращения: 15.02.2018).