БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Хованскова В.С., Румянцев К.Е., Хованскоов С.А.* Метод повышения защиты работоспособности распределенных вычислений в компьютерных сетях // Известия ЮФУ. Технические науки. – 2012. – № 4 (129). – С. 102-107.
2. *Хованскоов С.А., Норкин О.Р.* Алгоритм повышения производительности распределенных сетевых вычислений // Информатизация и связь. – 2011. – № 3. – С. 96-98.
3. *Литвиненко В.А., Хованскоов С.А.* Решения задач путем организации распределенных вычислений в сети // Известия ЮФУ. Технические науки. – 2008. – № 3 (80). – С. 16-21.
4. *Хованскоов С.А., Норкин О.Р.* Алгоритмическая оптимизация конфигурации системы децентрализованных вычислений // Телекоммуникации. – 2012. – № 11. – С. 2-5.
5. *Хованскоов С.А.* Организация распределенных вычислений с иерархической структурой связей // Информационное противодействие угрозам терроризма. – 2007. – № 9. – С. 170-178.
6. *Литвиненко В.А., Хованскоов С.А.* Алгоритм оптимизации параметров компьютерной сети для уменьшения времени решения задачи на основе мультиагентной системы // Известия ЮФУ. Технические науки. – 2007. – № 2 (77). – С. 186-190.
7. *Хованскоов С.А., Литвиненко В.А., Норкин О.Р.* Организация распределенных вычислений для решения задач трассировки // Известия ЮФУ. Технические науки. – 2010. – № 12 (113). – С. 48-55.
8. *Калашников В.А., Трунов И.Л., Хованскоов С.А.* Параллельный алгоритм размещения на многопроцессорной вычислительной системе // Известия ЮФУ. Технические науки. – 1997. – № 3 (6). – С. 181-184.

Статью рекомендовал к опубликованию д.т.н. С.Г. Капустян.

Румянцев Константин Евгеньевич – Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Южный федеральный университет»; e-mail: rke2004@mail.ru; 347900, г. Таганрог, ул. Чехова, 2; тел.: 88634328725; кафедра ИБТКС; зав. кафедрой; д.т.н.; профессор,

Хованскоов Сергей Андреевич – e-mail: sah59@mail.ru; тел.: 88634642530; кафедра ИБТКС; к.т.н.; доцент.

Хованскова Вера Сергеевна – e-mail: wepok@mail.ru; тел.: 88634676616; студентка.

Rumyantsev Constantine Evgen'evich – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University"; e-mail: rke2004@mail.ru; 2, Chekhov street, Taganrog, 347900, Russia; phone: +78634328725; the department of IBTKS; head the department; dr. of eng. sc.; professor.

Khovanskov Sergey Andreevich – e-mail: sah59@mail.ru; phone: 88634642530; the department of ISTCN; cand. of eng. sc.; associate professor.

Khovanskova Vera Sergeevna – e-mail: wepok@mail.ru; phone: +78634676616; student.

УДК 004.056

Е.Н. Ефимов, Г.М. Лапицкая

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И БИЗНЕС-ПРОЦЕССЫ КОМПАНИИ

Цель исследования показать, что информационная безопасность должна создаваться и существовать в рамках достижения бизнес-целей компании. При этом бизнес-процессы являются первоисточником данных для организации информационной безопасности компании.

При разработке стратегии управления информационной безопасностью предложена комплексная диагностика состояния компании с помощью SWOT-анализа с условной количественной оценкой результатов, полученной с помощью метода анализа иерархий.

Идентификация рисков необходима для оценки значимости угроз и построения системы безопасности. Анализ показал, что риски бизнес-процессов компании группируются в следующие категории: риски при проектировании, риски при реинжиниринге и риски в процессе использования бизнес-процессов.

Автоматизировать процессы информационной безопасности компании целесообразно с помощью системы класса GRC (Governance, Risk management and Compliance), которые сегодня рассматриваются как один из эффективных способов управления информационными технологиями и информационной безопасностью. Систему GRC при этом целесообразно комплексировать с системами класса Business Process Management, предназначенных для управления бизнес-процессами компании.

Бизнес-цели; информационная безопасность; бизнес-процессы.

E.N. Efimov, G.M. Lapitskaya

INFORMATION SECURITY AND BUSINESS PROCESSES OF THE COMPANY

The Purpose of the study to show that information safety must be created and exist within the framework of achievement business-integer to companies. At business-processes are a firsthand given for organization of information safety to companies.

At development of the strategies of management information safety is offered complex diagnostics of the condition to companies by means of SWOT-analysis with conditional quantitative estimation result, got by means of method of the analysis hierarchy.

The Identification risk required for estimation of value of the threats and buildings of the system to safety. The Analysis has shown that risks business-processes to companies are grouped in the following categories: risks when designing, risks under reengineering and risks in process of the use business-processes.

Automate the processes to safety to companies reasonable by means of systems of the class GRC (Governance, Risk management and Compliance), which are today considered as one of the efficient ways of management information technology and information safety. The Systems GRC herewith necessary complex with system of the class Business Process Management, intended for governing business-process to companies.

Business-purposes; information safety; business-processes.

Постановка проблемы. Информационная безопасность должна создаваться и существовать в рамках достижения бизнес-целей компаний. Эффективное ведение бизнеса невозможно без использования современных информационных технологий (ИТ), которые используются для поддержки практически всех бизнес-процессов современной компании. Однако сегодня очевидна тенденция: информационная безопасность из защиты конкретных сетей, серверов, информационных ресурсов, превращается в безопасность бизнес-процессов компаний, поддерживаемых ИТ. Это предполагает наличие двух взаимозависимых направлений обеспечения безопасности компании: с одной стороны – эффективная работа бизнеса в части функционирования бизнес-процессов; с другой – нормальное функционирование поддерживающей ИТ-инфраструктуры. В настоящее время не сложилось единого подхода к информационной безопасности именно в данном контексте.

Для понимания основных проблем безопасности компании целесообразно выполнить тщательный анализ внешней и внутренней среды бизнеса, выделить те компоненты, которые действительно имеют значение, провести сбор и отслеживание информации по каждому компоненту и на основе оценки реального положения выяснить состояние компании и причины этого положения. Точная, комплексная, своевременная диагностика состояния компании – первый этап в разработке стратегии управления безопасной деятельностью.

Самый распространенный способ оценки стратегического положения компании – *SWOT*-анализ[1]. Матрица *SWOT*-анализа может быть представлена в виде следующей совокупности:

$$\boldsymbol{SWOT = <St, W, Op, Th>,}$$

где *St* (*Strengths*) – множество сильных сторон организации, $St = (St1, St2, \ldots, Stnst)$; *W* (*Weaknesses*) – множество слабых сторон организации, $W = (W1, W2, \ldots, Wnw)$; *Op* (*Opportunities*) – множество возможностей организации, $Op = (Op1, Op2, \ldots, Opnop)$; *Th* (*Threats*) – множество угроз организации, $Th = (Th1, Th2, \ldots, Thnth)$.

При этом важно понимать, что сильные $St = (St1, St2, \ldots, Stnst)$ и слабые $W = (W1, W2, \ldots, Wnw)$ стороны – это те составные части деятельности компании, которые она может контролировать, а возможности $Op = (Op1, Op2, \ldots, Opnop)$ и угрозы $Th = (Th1, Th2, \ldots, Thnth)$ – это те факторы, которые находятся вне контроля компании и могут повлиять на процесс ее развития [5].

Результаты *SWOT*-анализа позволяют сформулировать стратегию безопасности компании на данном этапе развития. Эта задача вряд ли может быть формализована, однако на основе этих данных может быть разработано множество стратегий организации $S = (S1, S2, \ldots, Sn)$.

Для условной количественной оценки *SWOT*-матрицы возможно использовать, например, метод анализа иерархий (МАИ). Данный метод обеспечивает реализацию наиболее эффективного способа оценки количественно неизмеримых, но вместе с тем важных, факторов для принятия обоснованных решений. Кроме того, метод работает с несогласованными суждениями и не требует, чтобы предпочтения потребителей или лица принимающего решение (ЛПР) соответствовали аксиомам полезности. МАИ позволяет сводить исследования сложных проблем к простой процедуре проведения последовательно парных сравнений [2].

В качестве примера рассматривались результаты *SWOT*-анализа действующего предприятия телекоммуникационной отрасли (ОАО «Телеком»), предоставляющего полный спектр услуг связи (проводная и беспроводная телефония, доступ в сеть Интернет, услуги радиосвязи, информационные услуги) на территории города и области (в статье не приводится). Вариант последующей оценки *SWOT*-матрицы с помощью МАИ представлен в табл. 1.

Таблица 1

Оценка *SWOT*-матрицы

	St	*W*	*Op*	*Th*	Вектор приоритетов	Нормализованный вектор
St	1	1	0,33	0,33	0,58	0,10
W	1	1	0,2	0,14	0,41	0,07
Op	3	5	1	0,2	1,32	0,24
Th	3	7	5	1	3,20	0,58

Индекс согласованности $ИС = 0{,}14$ и отношение согласованности $ОС = 15{,}58 < 20$ % показывают удовлетворительную согласованность оценок ЛПР.

Значения нормализованного вектора лежат в пределах [0,1], поэтому результаты экспертных расчетов могут трактоваться следующим образом: “угрозы” организации значительны ($Th = 0{,}58$), “возможности” организации для решения проблем удовлетворительны ($Op = 0{,}24$), “силы” организации для преодоления проблем посредственны ($St = 0{,}1$), “слабости” организации незначительны ($W = 0{,}07$).

[1] *SWOT* – это аббревиатура, включающая начальные буквы четырёх английских слов: *strength* («сила»), *weakness* («слабость»), *opportunities* («возможности»), и *threats* («угрозы»)

Такой взгляд на проблему безопасности компании позволяет конкретизировать ее цель и задачи, объекты и угрозы, выработать план мероприятий по снижению рисков бизнес-процессов и произвести оценку эффективности проведенных мероприятий.

В связи с определенной спецификой исследования информационной безопасности с точки зрения безопасности бизнес-процессов компании необходимо вначале выполнить идентификацию рисков бизнес-процессов. Целью идентификации рисков является оценка подверженности компании угрозам, которые могут нанести существенный ущерб. Для сбора информации о рисках производится анализ бизнес-процессов компании и опрос экспертов предметной области. Результатом данного процесса является классифицированный перечень всех потенциальных рисков.

Идентификация рисков бизнес-процессов. Бизнес-процесс можно представить как преобразование:

$$P\ (X, R, F, Z, G) \rightarrow Y,$$

где P — процесс, имеющий вид множества действий $P = \{ D_1, D_2, \ldots, D_p\}$; $X = \{ X_1, X_2,\ldots, X_i\}$ – входные потоки бизнес-процесса и их поставщики; $Y = \{ Y_1, Y_2,\ldots, Y_j\}$ – выходные потоки бизнес-процесса и их потребители; $R = \{ R_1, R_2,\ldots, R_k\}$ – множество ресурсов, используемых для выполнения бизнес-процесса (технические, материальные, информационные); $F = \{ F_1, F_2,\ldots, F_n\}$ – множество функций, реализуемых в бизнес-процессе; $Z = \{ Z_1, Z_2,\ldots, Z_m\}$ – множество участников и исполнителей бизнес-процесса; $G = \{ G_1, G_2,\ldots, G_l\}$ – границы и интерфейсы процесса.

Из данного определения видно, что бизнес-процессы являются первоисточником данных для организации информационной безопасности компании.

Вначале необходимо определить объекты защиты, т.е. что и от каких угроз следует защищать. К объектам защиты, безусловно, относятся *информация, бизнес-процессы и материальные ресурсы* компании.

Очевидным началом работ по информационной безопасности сегодня признается классификации данных компании. Классификация — процесс сложный, требующий немало времени и средств. Для того, чтобы классификация была эффективной, ее необходимо постоянно поддерживать и актуализировать. Целесообразность классификации заключается в том, что она позволяет определить все места хранения информации и выявить ту информацию, которую следует защищать. Это позволяет минимизировать количество конфиденциальной информации. При проведении классификации выявляются документы, бывшие когда-то секретными, но теперь уже потерявшие свою актуальность. Их можно отправить в архив или безвозвратно удалить.

Информационные активы (ИА) как объекты защиты требуют поддержания целостности, доступности и, если требуется, конфиденциальности информации в бизнес-системах. Проведенный анализ возможных угроз показал, что информационная инфраструктура должна обладать свойством защищенности информации, используемой в бизнес-процессах, т.е. обеспечивать защиту от несанкционированного (преднамеренного или случайного) получения, изменения, уничтожения или использования коммерческой, служебной или технологической информации. С учетом наличия компонентов бизнес-процесса, а также их взаимосвязей, к потенциально опасным ситуациям относятся: несанкционированный доступ нарушителей (не владельцев и участников процессов) к информации, хранящейся и обрабатываемой в средствах автоматизации, с целью ознакомления, искажения или уничтожения. При этом, точками входа могут быть интерфейсы и границы процесса, а также информация, необходимая для реализации функций (операций, процедур) процесса; перехват информации при ее приеме (передаче) по каналам связи

(сети) функциями процесса, а также за счет хищения носителей информации; уничтожение (изменение, искажение) информации за счет случайных помех, сбоев технических (программных) средств при передаче, хранении и обработке информации; несанкционированное влияние на бизнес-процесс нарушителей из числа владельцев и (или) участников процесса [3].

Анализ предметной области показал, что целесообразно идентифицировать риски бизнес-процессов компании на всех основных стадиях их жизненного цикла: на этапах проектирования, реинжиниринга и в процессе использования бизнес-процессов.

Идентификация рисков при проектировании и реинжиниринге бизнес-процессов. Даже первоначальное описание основных бизнес-процессов компании приносит как ощутимые результаты повышения эффективности работы, так и возможные потери (риски). Это, прежде всего, риски из-за ошибок при проектировании процессов: ошибки незавершенности (наличие пробелов в описании процесса); ошибки несоответствия (неадекватного использования информационных ресурсов в различных частях процесса, что приводит к искаженному восприятию информации или к неясности указаний); ошибки иерархической или «наследственной» несовместимости (наличие конфликта между основными и последующими процессами). Очевидно, следует допустить и наличие иных видов ошибок.

Следующий ряд рисков возникает из-за ошибок в методологии описания процессов (или парадигмы «*методология — модель — нотация — средства*»): при отображении функций системы; процессов, обеспечивающих выполнение функций; данных и организационных структур, обеспечивающих выполнение функций; материальных и информационных потоков в ходе выполнения функций.

Далее следует отметить риски, возникающие из-за несоответствия топологии процесса, не позволяющие добиться максимально понятного течения процесса, отражающего при этом либо реальное положение вещей, либо оптимальное с учетом загрузки исполнителей, доступности ресурсов или других обстоятельств. Анализ ошибок топологии процесса может проводиться в несколько итераций. В результате анализируемый процесс может кардинально измениться. Например, функции, которые раньше выполнялись последовательно друг за другом, будут выполняться параллельно. Безусловно, что при этом не должна исказиться логика процесса и получаемый результат.

Идентификация рисков при использовании бизнес-процессов. Операционный риск можно определить как риск прямых или косвенных убытков в результате неверного исполнения бизнес-процессов, неэффективности процедур внутреннего контроля, технологических сбоев, несанкционированных действий персонала или внешнего воздействия. Операционный риск критичен для процессов, характеризующихся значимостью для деятельности организации в целом, большим числом транзакций в единицу времени, сложной системой технической поддержки. Выделяемые обычно риск-факторы аналогичны показателям состояния внутренней операционной среды и бизнес-процессов – объем операций, оборот, процент ошибочных действий. Управление операционными рисками осуществляется построением прозрачных и управляемых бизнес-процессов, правильной организационной структурой с опорой на экспертное знание [1].

Для решения задач устранения операционных рисков бизнес-процессов может быть использована система *lean production* (бережливое производство) – концепция менеджмента, созданная на основе производственной системы *Toyota.* Цель *lean* – идентифицировать, проанализировать и устранить потери в производственных процессах [4]. В соответствии с концепцией *lean* в бизнес-процессах возникает восемь видов потерь: неиспользование потенциала сотрудников; потери

от перепроизводства; потери на транспортировку; потери от брака, излишних отходов и переделок; потери на обслуживание запасов; потери на перемещениях и движениях персонала; потери от простоев; потери из-за чрезмерной обработки. Потери в этом случае рассматриваются как операции, на которые затрачиваются временные и материальные ресурсы, без добавления ценности товару или услуге для конечного потребителя.

Так, к примеру, необходима защита от противоправных действий персонала, выполняющего бизнес-процессы, несанкционированного воздействия на поставщиков, объемы и сроки поставки ресурсов; регламент выполнения бизнес-процессов, в т.ч. регламент внутренних и внешних интерфейсов; технологию выполнения бизнес-процессов и прочее.

Описание бизнес-процессов, их моделирование, последующий контроль и анализ выполнения – постоянная и последовательная деятельность по устранению операционных рисков, а следовательно и потерь.

Автоматизировать процессы информационной безопасности компании можно с помощью систем класса *GRC* (*Governance, Risk management and Compliance*), которые рассматриваются сегодня как один из эффективных способов управления информационными технологиями и информационной безопасностью.

GRC это взгляд на управление чем-либо с трёх точек зрения: высшего руководства (*Governance*), управления рисками (*Risk management*) и соответствия требованиям (*Compliance*). Результатом обработки информации о деятельности всех подразделений компании становятся наглядные отчеты, сформулированные в терминах бизнеса.[2]

Например, модуль *Enterprise Management* продукта *RSA Archer eGRC* позволяет выполнить инвентаризацию и классификацию активов компании, создать единый реестр взаимоувязанных между собой активов, включая информационные и технологические активы, бизнес-процессы, товары и услуги, подразделения и отдельные бизнес-единицы, производственные помещения и оборудование, контакты с ответственными работниками компании, партнерами и поставщиками. Для каждого актива определяется его владелец и ценность для компании. Результаты данной работы могут использоваться при дальнейшем проведении процедуры оценки рисков информационной безопасности. Интеграция с системами управления уязвимостями *SIEM* или *DLP* позволяет установить приоритет устранения уязвимостей и нейтрализации инцидентов в отношении каждого конкретного актива. [3]

Однако реализовать все функции *GRC* в контексте безопасности бизнес-процессов с помощью одного, пусть даже хорошего, ИТ−решения практически невозможно. Система, которая может помочь в решении задач этой концепции, должна быть такая же комплексная, как и сами задачи *GRC*.[4] Для комплексирования с *GRC*-системой целесообразно использовать системы класса *Business Process Management (BPM), Business Performance Management и Business Intelligence*, предназначенные для автоматизации и управления бизнес-процессами. Диаграмма взаимосвязи бизнес-процессов и основных субъектов информационной безопасности компании в нотации *UML* приведена на рис. 1.

[2] Евгений Безгодов Что такое *GRC* и чем это может быть полезно для информационной безопасности? [Электронный ресурс] *http://ru.deiteriy.com/what_is_grc_and_its_ usability_in_information_security/.*

[3] *GRC* – путь к оптимизации процессов управления ИБ //Банковское обозрение №9 (176) Сентябрь 2013 [электронный ресурс] *http://www.bosfera.ru/bo/put-k-optimizatsii-protsessov*

[4] Концепция *GRC* стала очередным этапом развития рынка ИБ [Электронный ресурс] *http://www.cnews.ru/reviews/free/security2008/articles/grc.shtml.*

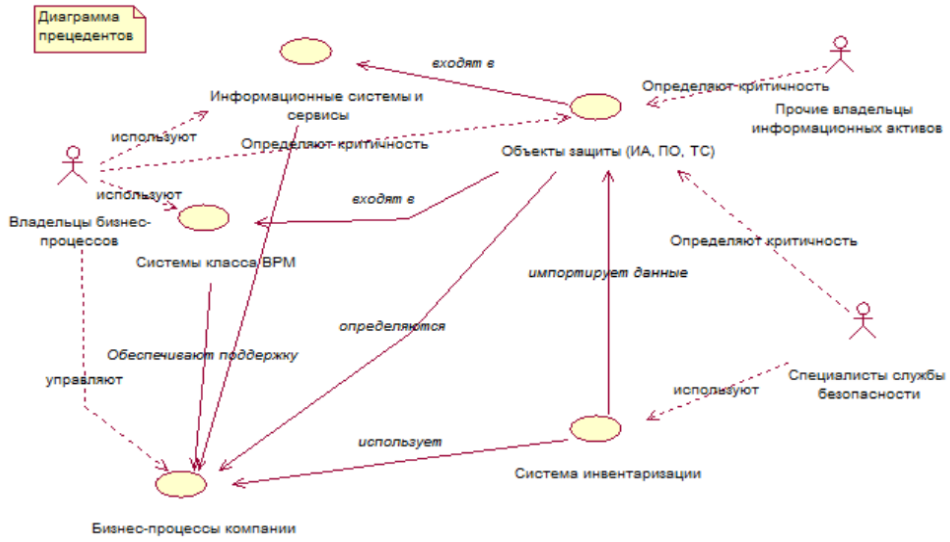

Рис. 1. Взаимосвязь бизнес-процессов и основных субъектов информационной безопасности компании

Взаимодействие бизнес-процессов компании и среды, создающей угрозы, прежде всего для бизнес-процессов, в рамках системы информационной безопасности приведено на диаграмме ниже (рис. 2).

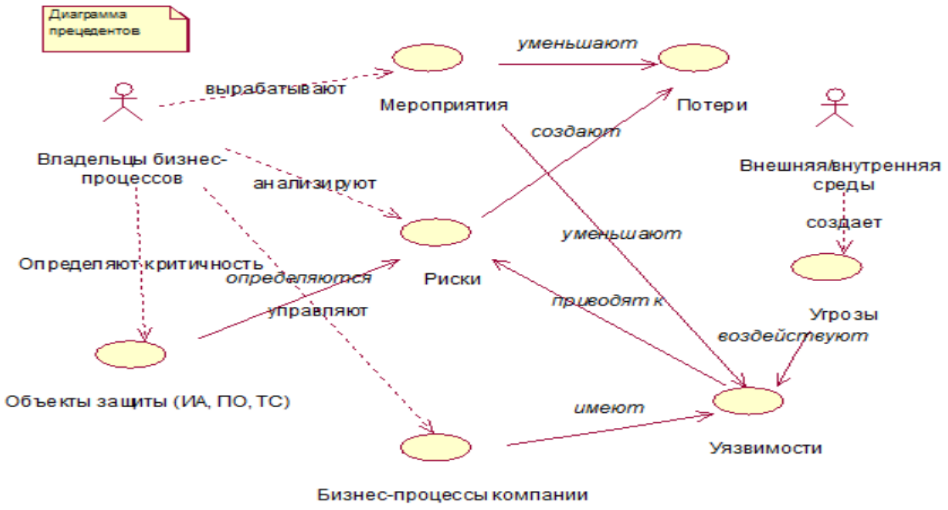

Рис. 2. Взаимодействие бизнес-процессов и среды, создающей угрозы

Основные выводы.

Комплексная диагностика состояния компании – первый этап в разработке стратегии управления информационной безопасностью, которую лучше всего выполнить с помощью *SWOT*-анализа с предлагаемой условной количественной оценкой.

Анализ показал, что бизнес-процессы являются первоисточником данных для организации информационной безопасности компании.

Обеспечение информационной безопасности бизнес-процессов следует начинать с разработки классификации данных, которая позволяет выявить информацию для защиты, минимизировать количество конфиденциальной информации, определить все места хранения информации, что может быть использовано для оптимизации бизнес-процессов в компании.

Анализ возможных рисков бизнес-процессов позволил установить следующие группы: *риски при проектировании, реинжиниринге и в процессе использования бизнес-процессов.*

Автоматизировать процессы информационной безопасности компании целесообразно с помощью системы класса *GRC* (*Governance, Risk management and Compliance*), которая должна комплексироваться с системами класса *Business Process Management, Business Performance Management* или *Business Intelligence*, предназначенные для автоматизации и управления бизнес-процессами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Каменнова М.С., Громов А.И., Ферапонтов М.М., Шматалюк А.Е.* Моделирование бизнеса. Методология *ARIS*. – М.: Весть-МетаТехнология, 2001.
2. *Саати Т.* Принятие решений. Метод анализа иерархий. – М.: Радио и связь, 1993.
3. *Стельмашонок Е.В.* Организация информационной защиты–бизнес-процессов // Прикладная информатика. – 2006. – № 2. – С. 42-57.
4. *Тимохин А.* Как найти все потери: практика применения методологии *lean* в НПО «ЭЛСИБ» // "БОСС" № 9, 2012.
5. *Ханова А.А.* Структурно-функциональная модель сбалансированной системы показателей при принятии управленческих решений // Вестник АГТУ Сер.: Управление, вычислительная техника и информатика. – 2012. – № 1. – С. 200-208.

Статью рекомендовал к опубликованию к.т.н. А.П. Лапсарь.

Ефимов Евгений Николаевич – Ростовский государственный экономический университет (РИНХ); e-mail: efimov46@mail.ru; 344002, г. Ростов-на-Дону, Б. Садовая, 69, комн. 306 а; тел.: 89525721917; кафедра информационных технологий и защиты информации; д.э.н.; профессор.

Лапицкая Галина Мелконовна – e-mail: gmlapickaya@mail.ru; тел.: 89286050143; кафедра информационных технологий и защиты информации; к.э.н.; профессор.

Efimov Evgeniy Nikolayevich – Rostov State Economic University; e-mail: efimov46@mail.ru; 69, B. Sadovaya street, room 306 a, Rostov-on-Don, 344002, Russia; phone: +79525721917; the department information technologies and information security; dr.ec. sc.; professor.

Lapickaya Galina Melkovna – e-mail: gmlapickaya@mail.ru; phone: +79286050143; the department information technologies and information security; cand.ec. sc.; professor.