

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ АНТИКРИЗИСНОГО УПРАВЛЕНИЯ ДЕЯТЕЛЬНОСТЬЮ ПРЕДПРИЯТИЙ

Получено: 01.03.2019; одобрено: 29.03.2019; опубликовано: 19.04.2019

УДК 658.15 JEL H12 DOI 10.26425/2658-3445-2019-1-52-59

Белоусов Виталий Андреевич

Старший преподаватель, ФГБОУ ВО «Государственный университет управления», Москва, Российская Федерация
e-mail: maryzver@gmail.com

Гончаров Валентин Николаевич

Д-р экон. наук, профессор, ГОУ ЛНР «Луганский национальный аграрный университет», г. Луганск, Луганская народная республика
e-mail: rector@lnau.su

АННОТАЦИЯ

В статье усовершенствованы теоретические подходы к управлению информационной безопасностью в контексте антикризисного управления предприятиями, предусматривающие разработку стратегии информационной безопасности для минимизации потерь от последствий кризиса. Основной целью стратегии является поддержание конфиденциальности, целостности и пригодности информации для осуществления эффективного антикризисного управления предприятиями. Среди стратегических направлений выделены организационное и инженерно-техническое обеспечение информационной безопасности. Стратегия организационного обеспечения включает анализ внешних и внутренних угроз, организацию работы с сотрудниками, документами, организацию режима и охраны, систематический контроль. Стратегия инженерно-технического обеспечения включает использование технических средств сбора, обработки, накопления и хранения конфиденциальной информации, защиту информации, систематический контроль. Реализация стратегических направлений позволит предприятиям как уменьшить возможные материальные убытки, так и сохранить конкурентные преимущества и позиции на рынке.

Доказано, что управление социально-экономической системой предприятия должно основываться на четкой информационной и коммуникационной платформе. Определены основные факторы возникновения кризиса предприятий: неразвитая система инновационных коммуникаций, отсутствие оптимального информационного обеспечения антикризисного управления, эффективной системы финансовой диагностики и низкий уровень трансфера технологий производства продукции. Обосновано, что преодоление кризисных явлений возможно через создание, развитие и поддержку инновационной инфраструктуры. Инновационная инфраструктура будет способствовать решению задач инновационной политики предприятий в рамках антикризисного управления. Предложено организационно-функциональное обеспечение информационно-инновационной составляющей антикризисного управления предприятиями с использованием коммуникационных инструментов инновационной инфраструктуры. Определены основные задачи функционирования инновационной инфраструктуры.

КЛЮЧЕВЫЕ СЛОВА:

Информационное обеспечение, антикризисное управление, предприятия, информационная безопасность, инфраструктура, коммуникации.

ЦИТИРОВАНИЕ

Белоусов В.А., Гончаров В.Н. Совершенствование информационного обеспечения антикризисного управления деятельностью предприятий//E-Management. 2019. № 1. С. 52–59.



THE ECOSYSTEM OF THE DIGITAL ECONOMY

IMPROVEMENT OF INFORMATIONAL SUPPORT OF CRISIS MANAGEMENT OF ENTERPRISES ACTIVITY

Received: 01.03.2019; approved: 29.03.2019; published: 19.04.2019

JEL CLASSIFICATION H12 DOI 10.26425/2658-3445-2019-1-52-59

Belousov Vitalii

Senior Lecturer, State University of Management, Moscow, Russia
e-mail: maryzver@gmail.com

Goncharov Valentin

Doctor of Economic Sciences, Professor, Lugansk National Agrarian University, Lugansk, Luhansk people's Republic
e-mail: rector@lnau.su

ABSTARCT

The article improves theoretical approaches to informational security management in the context of crisis management of enterprises, which include developing an informational security strategy to minimize losses from the effects of the crisis. The main goal of the strategy is to maintain the confidentiality, integrity and availability of information for the implementation of effective crisis management of enterprises. Organizational, engineering and technical support of informational security have been highlighted among the strategic areas. The strategy of organizational support includes the analysis of external and internal threats, the organization of work with employees, the organization of work with documents, the organization of the regime and protection, systematic control. The strategy of engineering and technical support includes the use of technical means of collecting, processing, accumulating and storing confidential information; protection of information; systematic control. Realization of strategic directions will allow enterprises to reduce both possible material losses and maintain competitive advantages and positions in the market.

It has been proved, that the management of the socio-economic system of the enterprise should be based on a clear informational and communicational platform. The main factors, responsible for the emergence of a crisis of enterprises have been determined: an undeveloped system of innovative communications, the lack of optimal informational support for crisis management, an effective system of financial diagnostics, and a low level of transfer of manufacture of products technologies. It has been substantiated, that overcoming the crisis phenomena is possible due to the creation, development and support of the innovative infrastructure. Innovative infrastructure will contribute to solving the problems of innovative policy of enterprises in the framework of crisis management. Organizational and functional support of the informational and innovative component of the crisis management of enterprises using communication tools of the innovative infrastructure has been proposed. The main tasks of the innovative infrastructure functioning have been defined.

KEYWORDS:

Informational support, crisis management, enterprises, informational security, infrastructure, communications.

FOR CITATION

Belousov B.A., Goncharov V.N. Improvement of informational support of crisis management of enterprises activity (2019) *E-Management*, 2 (1), pp. 52–59. doi: 10.26425/2658-3445-2019-1-52-59



В условиях роста информационной насыщенности экономики большое значение приобретает информационное обеспечение эффективной деятельности предприятия. Информация становится важным фактором обеспечения движения товара от производителя к потребителю [Андреева, 2012; Рудакова Т.А., Рудакова О.Ю., 2010].

По нашему мнению, информационный кризис – нарушение функционирования предприятия, возникшее в результате неэффективного информационного обеспечения элементов организационной структуры, искажения и нежелательного разглашения информации о предприятии сотрудниками.

Засвидетельствовано практикой – доверие потребителей и инвесторов оценивается прибылью. Важное значение при этом приобретают инструменты информационного обеспечения, а именно интернет-технологии. Наличие веб-сайта предприятия в Интернете предоставляет следующие преимущества: возможность найти предприятие из любой точки мира, обратная связь с конечными потребителями и инвесторами, повышение имиджа и репутации.

Для предотвращения кризисных ситуаций предприятие постоянно должно изучать тенденции изменений показателей и прогнозировать их; вести систематический управленческий учет производства и реализации готовой продукции. Именно поэтому возникает необходимость разработки программного обеспечения для учета расходов, готовой продукции; создания баз данных надежных и ненадежных партнеров (обработка дебиторской задолженности) и потребителей, создания и поддержания инфраструктуры трансфера инновационных технологий производства качественной и конкурентоспособной продукции.

Системная оценка антикризисного управления предприятий требует проведения финансово-экономической диагностики в рамках обеспечения надежной и качественной информации для принятия необходимых управленческих решений.

В рыночных условиях хозяйствования важную роль играет антикризисная система управления, которая позволяет на начальном (первом) этапе оценить реальное состояние социально-экономической системы, сформировать аналитическую базу и определить глубину кризисной ситуации. Тогда как в менеджменте диагностика является важным элементом функции контроля, который позволяет оценить степень отклонения и разработать соответствующие меры. Таким образом, нами сделан вывод, что процесс диагностики обеспечивает процесс управления необходимой информацией, которая позволяет принимать антикризисные решения.

Важным фактором возникновения кризиса предприятий является неразвитая система инновационных коммуникаций: отсутствие оптимального информационного обеспечения антикризисного управления и низкий уровень трансфера технологий производства продукции. Исследования показывают, что на информационные технологии опираются все процедуры антикризисного управления [Андреева, 2012; Белоус, Петропавлова, 2014; Рудакова Т.А., Рудакова О.Ю., 2010]. Таким образом, вопросы взаимодействия антикризисного управления и информационных технологий являются актуальными.

Учитывая, что в настоящее время экономический потенциал предприятий все в большей степени определяется уровнем развития информационной структуры, пропорционально растет потенциальная уязвимость от информационных воздействий. Поэтому руководству современного предприятия крайне необходимо в системе антикризисного управления обеспечить защиту информационных потоков, что является необходимым условием выживания и повышения уровня эффективности хозяйственной деятельности.

Глобальная распространенность распределенной вычислительной среды, облачные технологии усиливают возможности электронного проникновения в рабочие компьютеры предприятий, предоставляет дополнительные возможности возникновения системного экономического кризиса. Хозяйственная деятельность современных предприятий невозможна без эффективной системы управления производством, предусматривает комплексную автоматизацию процессов сбора, передачи, хранения экономической информации и принятия управленческих решений. В связи с этим приобретает актуальность проблема обеспечения информационной безопасности в контексте антикризисного управления предприятиями.

Выявлено, что с появлением компьютерных сетей отсутствие физического доступа к компьютеру не дает гарантию целостности и защищенности экономической информации. Наиболее существенными для современных предприятий последствия нарушения информационной безопасности – экономические и имиджевые потери [Андреева, 2012; Жариков и др., 2009; Камышев, 2009]. Это:

- раскрытие коммерческой информации – может привести к серьезным прямым убыткам на рынке;
- известие о краже большого объема информации – влияет на репутацию, приводя к потерям в объемах коммерческих операций.
- конкуренты могут воспользоваться кражей информации, если и осталась незамеченной, для того чтобы полностью разорить предприятие, навязывая ему фиктивные или сознательно убыточные сделки.
- подмена информации как на этапе передачи, так и на этапе сохранения на предприятии – может привести к огромным убыткам;
- многократные успешные информационные атаки на предприятие – снижают доверие к фирме у клиентов, что сказывается на объеме доходов.

В системе антикризисного управления предприятием следует выделить важную составляющую информационную подсистему.

Но существующие стандарты, документы, коммуникационные антикризисные инструменты на их основе не дают ответов на ряд ключевых вопросов: как создать информационную систему, чтобы она была защищена на необходимом уровне; как практически сформировать режим экономической безопасности и поддерживать его в условиях постоянно меняющегося внешнего окружения и структуры самой системы; реальный уровень информационной безопасности и насколько эффективна система защиты экономической и управленческой информации.

Системный подход в создании механизмов защиты информационных систем требует наличия следующих положений: понятие системности заключается не просто в создании соответствующих механизмов защиты от факторов кризиса, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла предприятия. При этом все средства, методы и мероприятия, которые используются для защиты информации объединяются в целостный механизм – систему антикризисного управления.

Уже в первых работах по защите информации были изложены основные постулаты, не потеряли своей актуальности и сегодня: абсолютную защиту создать нельзя; система информационной безопасности должна быть комплексной; должна быть такой, что адаптируется к рыночным условиям, которые постоянно меняются.

Во-первых, система информационной безопасности должна быть именно системой, а не простым, во многом случайным и хаотичным набором некоторых управленческих технологий, технических и организационных мероприятий, как это чаще всего наблюдается на практике. Во-вторых, системный подход к защите экономической и управленческой информации должен применяться, начиная с подготовки технического задания и заканчивая оценкой эффективности и качества системы информационной безопасности в пределах антикризисного управления.

К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания лиц, принимающих решения в современных системах антикризисного управления.

Сегодня менеджеры, экономисты, производители, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности. Это обусловлено тем, что в ближайшие период времени нам придется жить в обществе (среде) информационных технологий, куда перекоچуют все социальные проблемы человечества, в том числе и вопросы экономической безопасности и антикризисного управления предприятиями.

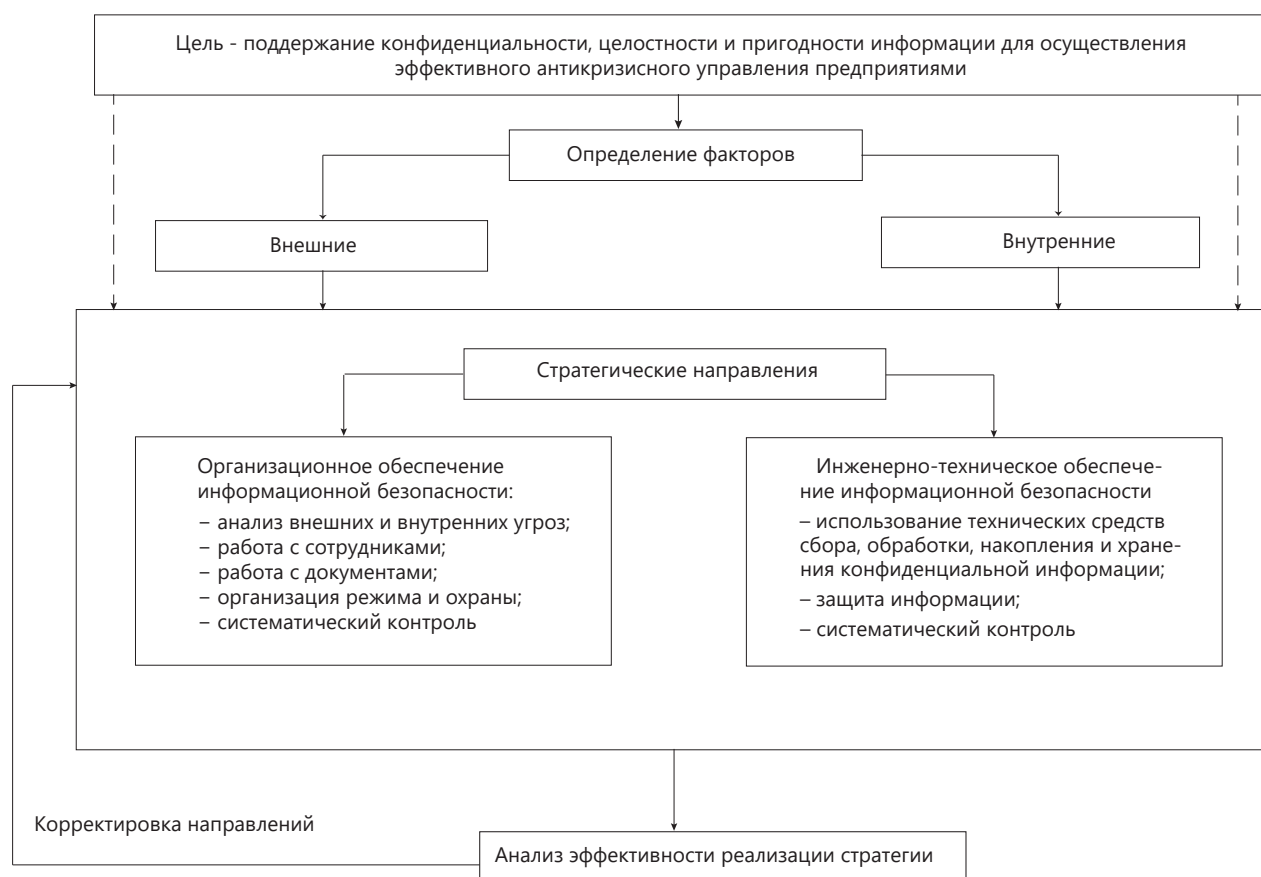
Однако следует признать, что на сегодняшний день в научных и практических кругах отсутствует методическая база, которая позволила бы сделать теоретические обобщения об обеспечении информационной безопасности в контексте антикризисного управления предприятиями.

По нашему мнению, система антикризисного управления предприятиями должна обеспечивать эффективное решение следующих задач: ранняя диагностика кризисных явлений в деятельности предприятий; срочное реагирование на вызовы и угрозы среды; изучение и реализация возможностей выхода предприятия из кризисного состояния.

Решение указанных задач становится необходимым условием успешной деятельности предприятий. Для их решения существуют современные информационные системы: информационные системы финансового управления и учета, информационные системы маркетинга, информационные системы по учету кадров и др. Эти системы осуществляют автоматизацию различных задач: хозяйственного учета готовой продукции, труда и заработной платы, расходов на производство, основных средств и нематериальных активов; управления

производством, запасами, портфелем заказов и др. Вместе с тем современные информационные системы помогают, с одной стороны, предотвратить риск на предприятии и эффективно используются при антикризисном управлении, с другой – они сами служат источником риска. Бизнес-процессы предприятия из-за своей зависимости от компьютерной техники являются достаточно уязвимыми. В связи с этим возникает необходимость в обеспечении информационной безопасности в контексте антикризисного управления предприятиями.

На основе положений, указанных выше, авторы предлагают стратегию обеспечения информационной безопасности. Основные содержательные элементы стратегии представлены на рисунке.



Составлено автором по материалам исследования

Рис. Содержание стратегии обеспечения информационной безопасности в контексте антикризисного управления предприятиями

Figure. Content of informational security strategy in the context of crisis management of enterprises

Стратегический план обеспечения информационной безопасности включает следующие этапы:

- разработка цели и стратегических целей поддержания конфиденциальности, целостности и пригодности экономической информации для осуществления эффективного антикризисного управления предприятиями;
- анализ внешней и внутренней среды, корректировка, при необходимости стратегических целей информационного обеспечения антикризисного управления предприятиями;
- разработка стратегических направлений поддержки информационной безопасности в системе антикризисного управления предприятиями;
- анализ реализации стратегического плана и корректировки стратегических направлений поддержки информационной безопасности в системе антикризисного управления предприятиями.

На рисунке проиллюстрированы факторы, причины, цели и стратегические направления обеспечения информационной безопасности. Среди причин разработки стратегии выделены угрозы информационной безопасности: угрозы, которые носят случайный характер и угрозы, обусловленные умышленными действиями людей. К ним относят официальную документацию предприятия, содержащую ложную, несвоевременную или неточную информацию. Угрозы, которые носят случайный характер: ошибки, возникающие

в результате работы аппаратуры или из-за недостаточной квалификации персонала. Угрозы, обусловленные умышленными действиями людей: хищения, разглашение информации, утечка экономической информации, несанкционированный доступ людей к информационным ресурсам, вывод из строя технического обеспечения, внедрение вирусов [Поносов, Пилипенко, 2013].

Основной целью стратегии является поддержание конфиденциальности, целостности и пригодности информации для эффективного антикризисного управления предприятиями. Информацией должны пользоваться только уполномоченные люди, она должна быть защищена от неправомерной модификации и всегда быть готова к использованию.

Среди стратегических направлений выделены следующие: организационное и инженерно-техническое обеспечение информационной безопасности. Стратегия организационного обеспечения включает анализ внешних и внутренних угроз, организацию работы с сотрудниками, документами, организации режима и охраны, систематический контроль.

Стратегия инженерно-технического обеспечения включает использование технических средств сбора, обработки, накопления и хранения конфиденциальной информации, защиту информации, систематический контроль.

Причинение вреда интеллектуальной собственности предприятия может привести к таким последствиям, как потеря позиций на рынке, потеря постоянных и временных конкурентных преимуществ или снижения стоимости торговой марки. Именно поэтому принимать решение следует на основе качественной оценки возможных эффектов.

Таким образом, доказана эффективность использования информационных технологий в процессе антикризисного управления. В связи с тем, что информационные технологии сами служат источником риска, отмечена необходимость обеспечения информационной безопасности в контексте антикризисного управления предприятиями.

Для поддержания конфиденциальности, целостности и пригодности информации в процессе эффективного антикризисного управления разработана стратегия обеспечения информационной безопасности в контексте антикризисного управления предприятиями. Реализация стратегических направлений позволит предприятиям уменьшить как возможные материальные убытки, так и сохранить конкурентные преимущества и позиции на рынке.

При анализе эффективности реализации стратегии обеспечения информационной безопасности в контексте антикризисного управления предприятиями следует учитывать, что основным эффектом, к которому стремится предприятие, является существенное уменьшение материального ущерба вследствие реализации существующих угроз информационной безопасности. Но не весь ущерб от реализации угроз информационной безопасности можно однозначно выразить в денежном выражении. Следовательно, обеспечение информационной безопасности требует внедрения инновационных решений и создания соответствующей антикризисной инновационной инфраструктуры для обеспечения антикризисных мер.

Особая роль в решении задачи преодоления кризисных явлений принадлежит инновациям. Создание информационной системы эффективного трансфера инновационных продуктов обеспечит адекватное реагирование на проблемные и кризисные явления национальной экономики на всех уровнях, в том числе на макроуровне, уровне предприятий.

Особая роль среди обслуживающих подсистем инновационной инфраструктуры принадлежит информационной подсистеме. Для повышения эффективности инновационного процесса необходима информационная поддержка процессов трансфера технологий, поиска партнеров для сотрудничества.

Среди причин, препятствующих эффективному освоению нововведений, является недостаточная информированность предприятий о существовании новых технологий и, в свою очередь, недостаточная информированность научных организаций о технологических нуждах предприятий. Именно поэтому возникает необходимость во внедрении современных информационных технологий для передачи и сохранения знаний и формирования инновационной инфраструктуры как элемента антикризисного управления предприятиями [Семке, 2012; Яснев и др., 2006].

Среди задач функционирования инновационной инфраструктуры нами выделены следующие:

- информационное обеспечение инновационной деятельности предприятий (создание базы данных и веб-сайта о спросе и предложении на инновационные продукты, предоставление доступа к ресурсу всем заинтересованным лицам);

- повышение внутренней эффективности производства и конкурентоспособности продукции предприятий;
- продвижения результатов инновационной деятельности на рынке;
- подготовка специалистов в области инновационного менеджмента;
- финансово-экономическое обеспечение инновационной деятельности (привлечение инвестиционных ресурсов из различных источников).

ЗАКЛЮЧЕНИЕ

Усовершенствованы теоретические подходы управления информационной безопасностью в контексте антикризисного управления предприятиями, предусматривающие разработку стратегии информационной безопасности для минимизации потерь от последствий кризиса. Важным фактором возникновения кризиса предприятий является неразвитая система инновационных коммуникаций: отсутствие оптимального информационного обеспечения антикризисного управления, эффективной системы финансовой диагностики и низкий уровень трансфера технологий производства продукции. Предложено организационно-функциональное обеспечение информационно-инновационной составляющей антикризисного управления предприятиями с использованием коммуникационных инструментов технологической платформы для повышения качества экономического состояния.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

- Андреева Т.А. (2012). Информационное обеспечение стратегического менеджмента предприятия//Информационная безопасность регионов. № 2. Режим доступа: <https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-strategicheskogo-menedzhmenta-predpriyatiya> (дата обращения: 14.02.2019).
- Белоус Е.В., Петропавлова Г.П. (2014). Антикризисное управление: зарубежный опыт и Российская практика//Экономика и экологический менеджмент. № 3. Режим доступа: <https://cyberleninka.ru/article/n/antikrizisnoe-upravlenie-zarubezhnyy-opyt-i-rossiyskaya-praktika> (дата обращения: 14.02.2019).
- Жариков В.В., Жариков И.А., Евсейчаев А.И. (2009). Антикризисное управление предприятием. Тамбов: Изд-во ТГТУ. 69 с.
- Поносов Е.В., Пилипенко Е.В. (2013). Модель совершенствования антикризисного управления на предприятиях промышленности//Актуальные вопросы современной науки. № 1. С. 117–124.
- Рудакова Т.А., Рудакова О.Ю. (2010). Информационное обеспечение антикризисного менеджмента в процедурах банкротства//Известия АлтГУ. № 1–2. Режим доступа: <https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-antikrizisnogo-menedzhmenta-v-protsedurah-bankrotstva> (дата обращения: 14.02.2019).
- Семке Ю.С. (2012). Сущность и основные элементы инновационной инфраструктуры//Вестник-Экономист ЗабГУ. № 4. С. 1–9.
- Яснев В.Н., Кокин А.С., Яшина Н.И. (2006). Финансовый менеджмент: монография. Н. Новгород: Нижегородский государственный университет им. Н.И. Лобачевского. 428 с.
- Камышев Э.Н. (2009). Информационная безопасность и защита информации: учебное пособие. Томск: ТПУ. 95 с.

REFERENCES

- Andreeva T.A. (2012). “Information support of the strategic management of the enterprise” [“Informatsionnoe obespechenie strategicheskogo menedzhmenta predpriyatiya”], Regional Information Security [Informatsionnaya bezopasnost' regionov], no. 2. Available at: <https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-strategicheskogo-menedzhmenta-predpriyatiya> (accessed 14.02.2019).
- Belous E.V. and Petropavlova G.P. (2014). “Crisis management: foreign experience and Russian practice” [“Antikrizisnoe upravlenie: zarubezhnyi opyt i Rossiiskaya praktika”], Economics and environmental management [Ekonomika i ekologicheskii menedzhment], no. 3. Available at: <https://cyberleninka.ru/article/n/antikrizisnoe-upravlenie-zarubezhnyy-opyt-i-rossiyskaya-praktika> (accessed 14.02.2019).
- Zharikov V.V., Zharikov I.A. and Evseichaev A.I. (2009), Crisis Management Company [Antikrizisnoe upravlenie predpriyatiem], Tambov State Tech. University, Tambov, Russia, 69 p.
- Ponosov E.V. and Pilipenko E.V. (2013), “Model of improving crisis management in industrial enterprises” [“Model' sovershenstvovaniya antikrizisnogo upravleniya na predpriyatiyakh promyshlennosti”], Actual issues of modern science [Aktual'nye voprosy sovremennoi nauki], no. 1, pp. 117–124.

Rudakova T.A. and Rudakova O.Yu. (2010), “Information support of crisis management in bankruptcy proceedings” [“Informatsionnoe obespechenie antikrizisnogo menedzhmenta v protsedurakh bankrotstva”], News of Altai State University [*Izvestiya AltGU*], no. 1–2. Available at: <https://cyberleninka.ru/article/n/informatsionnoe-obespechenie-antikrizisnogo-menedzhmenta-v-protsedurah-bankrotstva> (accessed 14.02.2019).

Semke Yu.S. (2012), “The essence and main elements of the innovation infrastructure” [“Sushchnost’ i osnovnye elementy innovatsionnoi infrastruktury”], Herald-Economist of the Transbaikal State University [*Vestnik-Ekonomist ZabGU*], no. 4, pp. 1–9.

Yasenev V.N., Kokin A.S. and Yashina N.I. (2006), Financial management [*Finansovyi menedzhment: monografiya*], Lobachevski State University of Nizhnii Novgorod, N. Novgorod, Russia, 428 p.

Kamyshev E.N. (2009), Information Security and Information Protection: Tutorial [*Informatsionnaya bezopasnost’ i zashchita informatsii: uchebnoe posobie*], Tomsk Polytechnic University, Tomsk, Russia, 95 p.