ОПУБЛИКОВАТЬ СТАТЬЮ

в изданиях НИЦ "Социосфера"

СОЦИОСФЕРА

- *Российский научный журнал*
- *ISSN 2078-7081*
- *РИНЦ*
- *Публикуются статьи по социально-гуманитарным наукам*

ПОДРОБНЕЕ

PARADIGMATA POZNÁNÍ

- *Чешский научный журнал*
- *ISSN 2336-2642*
- *Публикуются статьи по социально-гуманитарным, техническим и естественно-научным дисциплинам*

ПОДРОБНЕЕ

СБОРНИКИ КОНФЕРЕНЦИЙ

- *Широкий спектр тем международных конференций*
- *Издание сборника в Праге*
- *Публикуются материалы по информатике, истории, культурологии, медицине, педагогике, политологии, праву, психологии, религиоведению, социологии, технике, филологии, философии, экологии, экономике*

ПОДРОБНЕЕ

III. INFORMATION AND COMMUNICATION INNOVATIONS AS A FACTOR IN THE EMPOWERMENT OF INTERPERSONAL RELATIONSHIPS

МЕТОДИКА ОЦЕНКИ ИНФОРМАЦИОННЫХ РИСКОВ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКОЙ ЛОГИКИ

Ю. П. Луговскова *Кандидат физико-математических наук, доцент,*

А. З. Султанханов *студент,*

Оренбургский государственный университет, г. Оренбург, Россия

Summary. One of the most significant problems of our time is the protection and security of information objects, which is closely related to the management of information risks, their analysis and evaluation. The relevance of this study is determined by the need to analyze information risks, identify development factors and the possibility of eliminating various threats to information security. The article offers a method for solving the problem of information risk analysis at various enterprises. A constructed fuzzy model of information risks is presented, with a description of various potential areas, which will allow optimizing the analysis process. This information risk model will significantly reduce the degree of human involvement, as well as reduce the time for time-consuming data processing for analysts and experts, in addition, it can be used in the information security management system. Various risk management methods and their main applications are also considered.

Keywords: risk assessment; risk management; fuzzy inference system; enterprise information security.

На сегодняшний день в производство и управление современных организаций внедряется все больше новых информационных технологий, что приводит к росту количества уязвимостей и увеличению возможностей доступа к информации. Со временем проблемы информационной безопасности очень быстро становятся главной задачей управления организацией, поскольку затрагивают функции её защиты. Появление проблем информационной безопасности приводит к необходимости измерения величины информационного риска. В результате анализа информационных рисков можно определить необходимую степень защиты и поддерживать на должном уровне безопасность организации [9], поэтому перед каждым предприятием, встает вопрос об организации системы защиты [4], которая бы позволила в полной мере обеспечить безопасность функционирования оборудования и информации в информационной системе предприятия.

Существует множество разновидностей угроз информационной системе. Важно проанализировать все риски с помощью разных методов диагностики [1, 5, 7, 10], которые помогут грамотно выстроить систему защиты от угроз в информационном пространстве.

Предложенный метод, основанный на разработке системы нечеткого вывода, реализует качественную оценку рисков информационной безопасности и позволяет принять управленческие решения по их предотвращению. В рамках представленной исследовательской работы реализуется решение следующих задач: разработка метода анализа информационных рисков; построение модели информационных рисков с помощью аппарата нечеткого моделирования; представление возможные контрмеры для предотвращения рисков.

1. МЕТОДОЛОГИЯ АНАЛИЗА ИНФОРМАЦИИ, НЕОБХОДИМОЙ ДЛЯ ОЦЕНКИ РИСКА

Анализ рисков – то, с чего должно начинаться построение любой системы информационной безопасности. Риск информационной безопасности состоит из четырех основных компонентов: ресурс, угроза, уязвимость и воздействие (влияние). Необходимо, чтобы группа анализа (группа людей, которая состоит из сотрудников организации, имеющих достаточные знания IT-области) идентифицировала ресурсы и провела анализ рисков для тех ресурсов, которые являются наиболее критичными для организации. Для каждого критического ресурса необходимо составить профили угроз, рассмотрев всевозможные их потенциальные источники (антропогенные, техногенные, стихийные), величины воздействий, вероятности реализации угроз [2]. За основу разработки профиля угроз взяты деревья угроз, составленные Лебедевой Ю. Г. [7].

Группа анализа рассматривает отношения среди критических ресурсов, угрозы этим ресурсам и уязвимости, которые могут быть использованы при реализации угроз. Далее производится оценка существующих рисков (например, как в данной исследовательской работе, с помощью нечеткого моделирования). На основании этой оценки создается стратегия защиты и план по уменьшению риска для критических ресурсов организации.

2. ПОСТРОЕНИЕ НЕЧЕТКОЙ ИНФОРМАЦИОННОЙ МОДЕЛИ РИСКА

При оценке рисков можно учитывать неограниченное число параметров. В рамках проведенное исследования риск определяется:

- вероятностью реализации угрозы, зависящей от потенциала угрозы и эффективности средств защиты;
- величиной воздействия угрозы, то есть величиной ущерба, наносимого ресурсам информационной системы, в случае осуществления угрозы безопасности.

В работе качественная оценка рисков информационной безопасности, осуществляется с помощью аппарата нечеткой логики [8], который

основан на использовании алгоритма Мамдани (Mamdani) и реализован в интерактивной среде математического пакета MATLAB.

2.1. Конструкция контроллера с нечеткой логикой

Рассмотрим схему нечеткого контроллера со структурой типа Mamdani с двумя входными и одной выходной лингвистической переменной. Входными переменными являются вероятность реализации угрозы и величина воздействия, выходная переменная – значение риска. Определим характеристики входных и выходной лингвистических переменных.

В качестве терм–множества входной лингвистической переменной «Вероятность реализации угрозы» используется множество T_1 = {"очень низкий", "низкий", "средний", "высокий", "очень высокий"} с функциями принадлежности, изображенными на рисунке 1.

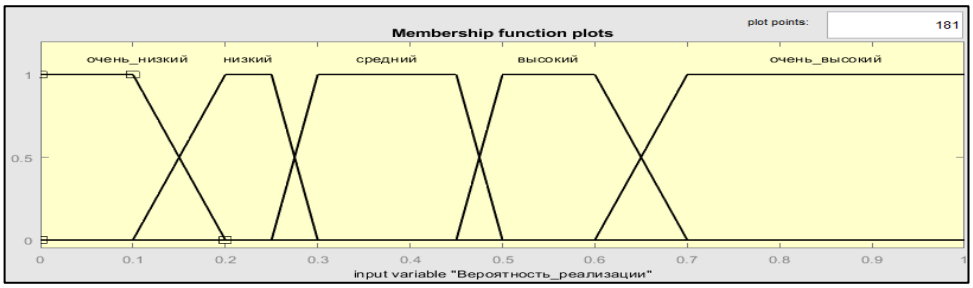


Рис. 1. **Функции принадлежности термов входной лингвистической переменной «Вероятность реализации угрозы»**

В качестве терм–множества входной лингвистической переменной «Величина воздействия» используется множество T_2 = {"очень низкий", "низкий", "средний", "высокий", "очень высокий"} с кусочно–линейными функциями принадлежности, изображенными на рисунке 2.

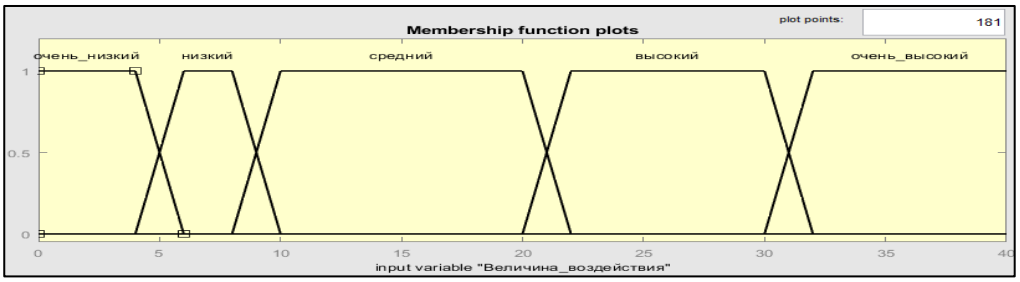


Рис. 2. **Функции принадлежности термов входной лингвистической переменной «Величина воздействия»**

Для входных лингвистических переменных были выбраны трапециевидные функции принадлежности, так как их ядро нечеткого множества включает в себя больший диапазон значений, относящихся к данным термам.

В качестве терм–множества выходной лингвистической переменной «Значение риска» используется множество T_3 = {"очень низкий риск", "низкий риск", "средний риск", "высокий риск", "очень высокий риск"} с функциями принадлежности, изображенными на рисунке 3.

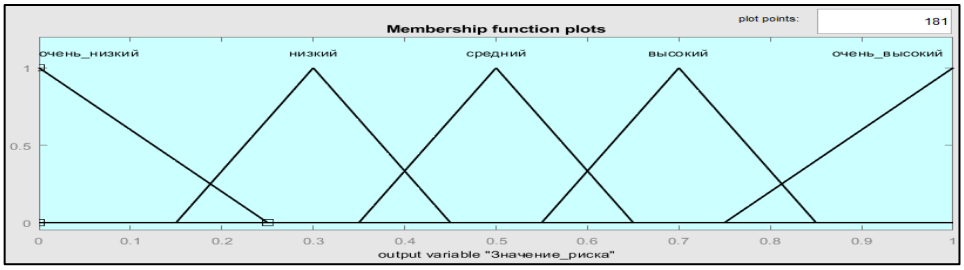


Рис. 3. **Функции принадлежности термов выходной лингвистической переменной «Значение риска»**

Процесс работы алгоритма нечеткой логики состоит из трех этапов: фаззификация, правила и дефаззификация. Процесс преобразования входных и выходных характеристик, включающий интервал вариации для каждой переменной и нечеткие множества, связанные с типом функции принадлежности, является методом фаззификации.

По определению входных и выходных нечетких множеств, всего было определено 25 правил "если-то". Лингвистические правила, связывающие входные и выходную переменные, детализированы на таблице, показанной на рисунке 4, представляющую собой множество правил нечетких продукций, связанных между собой логической конъюнкцией. По вертикали расположены термы входной лингвистической переменной «Величина воздействия», а по горизонтали входной лингвистической переменной «Вероятность реализации угрозы», на пересечениях этих терм определены термы выходной лингвистической переменной «Значение риска».

Величина воздействия угрозы					
очень высокая	СР	ВР	ОВР	ОВР	ОВР
высокая	НР	СР	ВР	ВР	ОВР
средняя	ОНР	НР	СР	ВР	ОВР
низкая	ОНР	НР	НР	СР	ВР
очень низкая	ОНР	ОНР	ОНР	НР	СР
Термы	очень низкая	низкая	средняя	высокая	очень высокая
	Вероятность реализации угрозы				

Рис. 4. **Лингвистические правила, связывающие входные и выходные переменные**

Вывод нечеткого логического контроллера получается с помощью дефаззификации, основанной на центроиде рассматриваемой области

2.2 Реализация нечеткой модели. Оценка риска в MATLAB

Графический интерфейс программы просмотра правил, представлен на рисунке 5. В нем можно выбрать определенные значения входных лингвистических переменных и наглядно увидеть, какие правила были задей-

ствованы, а также получить точное значение выходной лингвистической переменной «Значение риска».

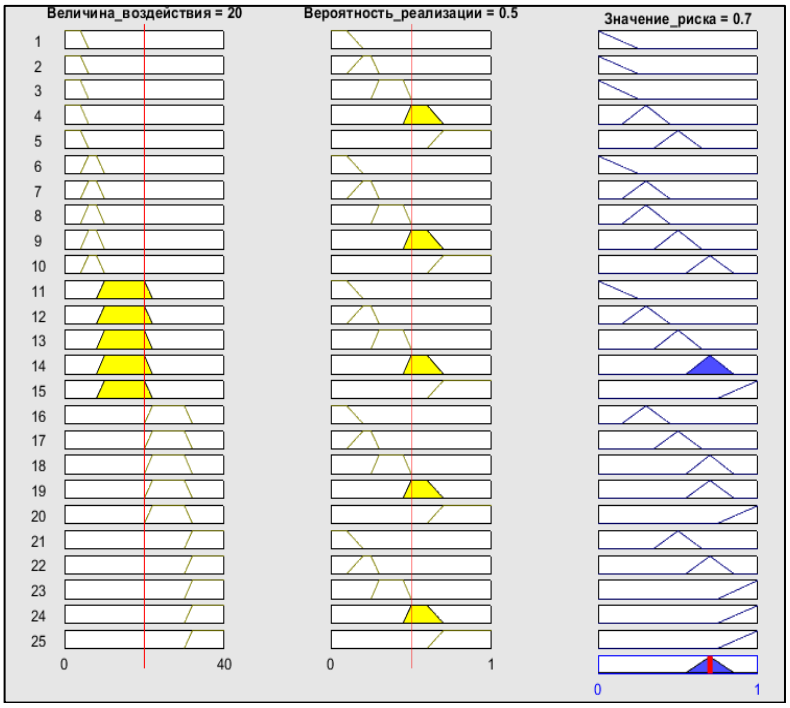


Рис. 5. **Графический интерфейс программы просмотра правил**

Процесс исследования и анализа разработанной нечеткой модели состоит из тестового выполнения нечетких выводов для различных значений входных переменных и оценки полученных результатов с целью внесения необходимых корректировок в случае несогласованности отдельных результатов.

На рисунке 6 представлена выходная поверхность контроллера, определяющая поверхность, позволяющую оценить величину риска в зависимости от величины воздействия и вероятности угрозы. Она представляет собой соотношение ввода-вывода в трехмерной конфигурации для предлагаемого нечеткого логического контроллера, где входы и выходы контроллера меняются кусочно-линейным способом.

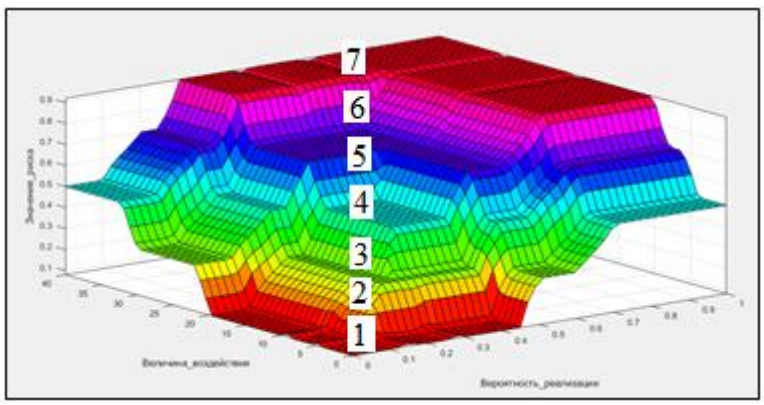


Рис. 6. **Нечеткая выходная поверхность**

Представленная нечеткая модель информационных рисков описывает различные потенциальные области [6]. В зоне 1 представлена безрисковая зона, в которой потери не ожидаются, в 2 и 3 отмечена зона допустимого риска, в пределах которой величина вероятных потерь невелика, в 4 и 5 показана зона критического риска, при котором необходимо применение контрмер, так как эти риски могут нанести огромные потери; в 6 и 7 изображена зона катастрофического риска, при котором вероятные потери могут достигать величины собственного капитала организации.

По результатам оценки необходимо ответить на два вопроса: являются ли существующие риски приемлемыми, и если нет, то какие меры защиты рентабельно использовать. Это означает, что оценка должна быть количественной, позволяющей проводить сравнение с заранее выбранными пределами допустимости.

3. МЕТОДИКА ПОЛУЧЕНИЯ КОЛИЧЕСТВЕННЫХ ЗНАЧЕНИЙ ВХОДНЫХ ПАРАМЕТРОВ

Для оценки риска входными параметрами являются: величина воздействия и вероятность реализации угрозы. В процессе получения количественных значений этих параметров участвует команда аналитиков и группа экспертов.

Для определения величины воздействия угрозы необходимо рассмотреть все важные для предприятия области воздействия, для этого участникам группы анализа предлагается пройти опрос, в котором приведены разные критерии для их оценки. Критерии, представленные на таблице 1 и таблице 2, составлены для рассмотрения некоторых из областей.

Таблица 1.

Ущерб финансовых потерь, связанных с восстановлением ресурсов

Степень ущерба	**Описание ущерба**	**Количество баллов**
Очень низкий	Ущербом можно пренебречь.	0 – 4
Низкий	Ущерб легко устраним, затраты на ликвидацию последствий реализации угрозы невелики.	4 – 8
Средний	Ликвидация последствий реализации угрозы не связана с крупными затратами и не затрагивает критически важные задачи.	8 – 12
Высокий	Ликвидация последствий реализации угрозы требует больших затрат и при этом затрудняется выполнение критически важных задач.	12 – 16
Очень высокий	Невозможность решения критически важных задач. Ликвидация последствий со значительными финансовыми инвестициями.	16 – 20

Таблица 2.

Ущерб репутации и деятельности организации в связи с недоступностью данных

Степень ущерба	Описание ущерба	Количество баллов
Очень низкий	Ущербом можно пренебречь.	0 – 4
Низкий	Финансовые операции не ведутся некоторое время. Положение на рынке и количество клиентов меняются незначительно.	4 – 8
Средний	Положение на рынке ухудшается. Потеря части клиентов	8 – 12
Высокий	Утрата на длительный период (например, до года) положения на рынке, а также большинства клиентов.	12 – 16
Очень высокий	Организация прекращает существование.	16 – 20

Итоговое значение воздействия является суммой баллов, полученных из результатов областей.

Для определения вероятности реализации угрозы создается группа экспертов, в которую могут входить, как члены группы анализа, так и сторонние эксперты. Группой экспертов проводится работа по численной оценке вероятностей реализации угроз, после чего можно перейти непосредственно к вычислению значения риска.

4. УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

На рисунке 7 изображена схема оценки риска для предпринятия возможных контрмер по их предотвращению, включающую 4 варианта обработки рисков [3]:

- снижение риска – целью выбора защитных мер является снижение вероятности и последствий проявления рисков информационной безопасности до уровня, приемлемого для данной организации;
- сохранение риска – если величина оцененных рисков информационной безопасности удовлетворяет критериям, нет необходимости внедрения дополнительных средств управления рисками, и оцененный риск может быть сохранен на прежнем уровне;
- избежание риска – если выявленные риски информационной безопасности считаются слишком высокими или затраты на осуществление действий по их обработке превышают выгоды, может быть принято решение полностью избежать риски путем отказа от осуществляемой деятельности или изменением условий осуществления данной деятельности;
- перенос риска – передача риска информационной безопасности другим сторонам, способным наиболее эффективно управлять им, по ре-

зультатам оценивания рисков – наилучший вариант, когда риск информационной безопасности неизбежен, трудно или слишком дорого добиться его снижения.

Основной метод управления рисками — это его снижение, изредка применяется избегание риска. Риски, характеризующиеся средним и высоким уровнем опасности, как правило передают или снижают. Риски низшего уровня опасности обычно сохраняют.

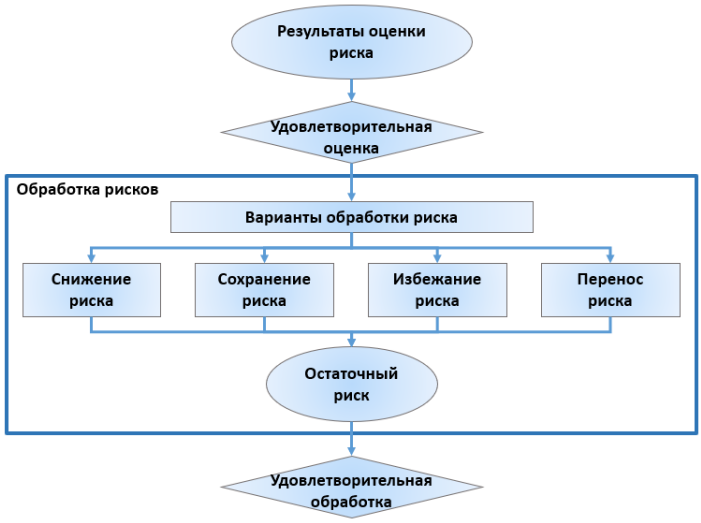


Рис. 7. **Схема оценки риска**

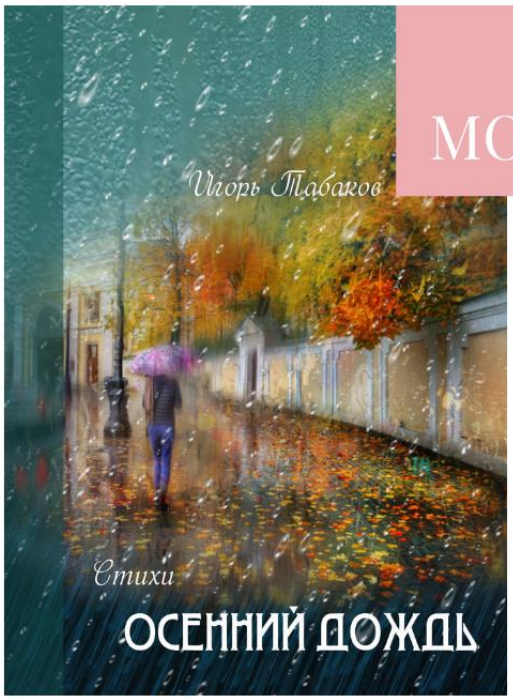
Данная работа посвящена анализу и оценке информационных рисков для различных организаций. В качестве основного инструмента для анализа используется нечеткая модель информационных рисков, позволяющая при качественных данных давать количественный результат.

Использование предлагаемого в статье способа является актуальным подходом к решению задачи анализа информационных рисков, а также имеет ряд преимуществ по сравнению с другими методиками, так как аппарата нечеткой логики строится на субъективной оценке, что позволяет подобрать более точные значения лингвистических переменных под определенную организацию, кроме этого, в области управления техническими системами нечеткое моделирование позволяет получать более адекватные результаты по сравнению с результатами которые основываются на использовании традиционных аналитических моделей и алгоритмов управления.

Библиографический список

1. Бирюк В.А., Булавка Ю.А., Иманов Р.Н. Методы оценки рисков в системе управления промышленной безопасностью предприятий нефтехимической промышленности // Вестник Университета гражданской защиты МЧС Беларуси. - 2018. - №4.
2. Вихорев С. В. Классификация угроз информационной безопасности. URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.
3. Киселева И.А., Искаджян С.О. Информационные риски: методы оценки и анализа // ИТпортал. - 2017. - №2 (14).

4. Коробкова О.К. Проблемные вопросы информационной безопасности организаций в рамках экономической безопасности РФ // Вестник Хабаровского государственного университета экономики и права. - 2021. - №1 (105).
5. Кривякин К.С., Изотова А.Р., Федоров В.М. Методический подход к оценке рисков информационной безопасности предприятия // ЭКОНОМИНФО. - 2018. - №2.
6. Куколко Е.С. Управление финансовыми рисками // ГИУСТ БГУ,2015.
7. Лебедева Ю.Г. Анализ и методика технологии управления информационными рисками // ГОУВПО ТвГУ - 2006.
8. Леоненков А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. - СПб.: БХВПетербург, 2005.
9. Лившиц И.И. К вопросу обеспечения безопасности промышленных систем // Научно-технический вестник информационных технологий, механики и оптики. - 2021. - №1.
10. Плетнев П.В., Белов В.М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады ТУСУР. - 2012. - №1-2 (25).

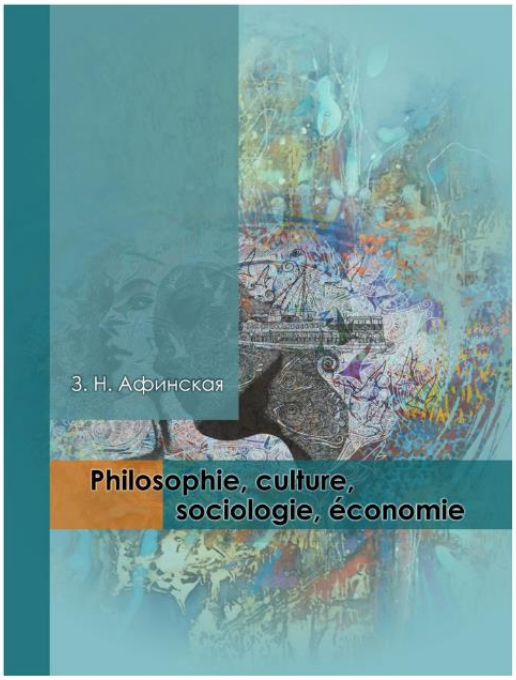


СРОЧНОЕ ИЗДАНИЕ МОНОГРАФИЙ И ДРУГИХ КНИГ

Два места издания Чехия или Россия.
В выходных данных издания
будет значиться
Прага: Vědecko vydavatelské centrum "Sociosféra-CZ"
или
Пенза: Научно-издательский центр "Социосфера"

РАССЧИТАТЬ СТОИМОСТЬ

- Корректура текста
- Изготовление оригинал-макета
- Дизайн обложки
- Присвоение ISBN



У НАС ДЕШЕВЛЕ

- Печать тиража в типографии
- Обязательная рассылка
- Отсулка тиража автору